Exam4 Training

QUESTION & ANSWER

Latest and valid Q&A

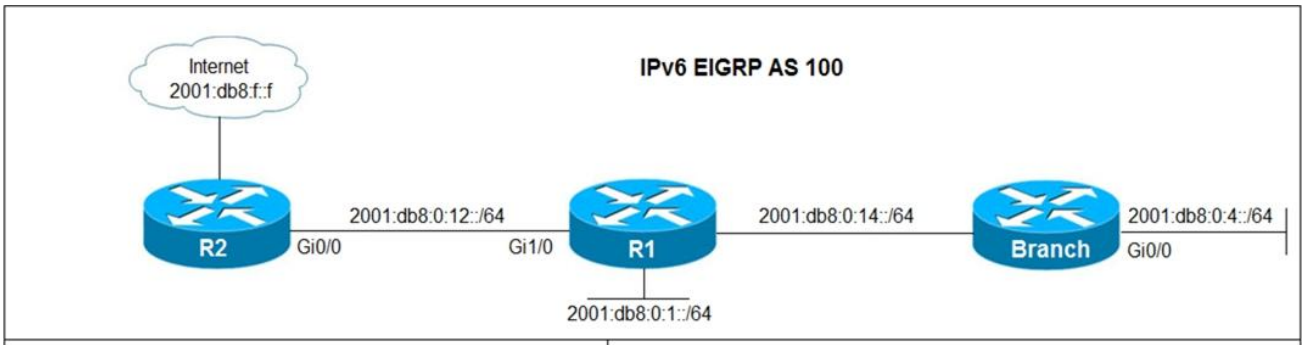
Once Fail, Full Refund

Exam : **300-410**

Title : Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)

Version : V22.02

1.Refer to the exhibit.




```
R1# show ipv6 eigrp topology
EIGRP-IPv6 Topology Table for AS(100)/ID(10.1.12.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 2001:DB8:0:4::/64, 1 successors, FD is 28416
       via FE80::C828:DFF:FEF4:1C (28416/2816), FastEthernet3/0
P 2001:DB8:0:1::/64, 1 successors, FD is 2816
       via Connected, GigabitEthernet0/0
P ::/0, 1 successors, FD is 2816
       via FE80::C821:17FF:FE04:8 (2816/256), GigabitEthernet1/0
P 2001:DB8:0:14::/64, 1 successors, FD is 28160
       via Connected, FastEthernet3/0
P 2001:DB8:0:12::/64, 1 successors, FD is 2816
       via Connected, GigabitEthernet1/0
```

```
Branch# show ipv6 eigrp topology
EIGRP-IPv6 Topology Table for AS(100)/ID(4.4.4.4)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 2001:DB8:0:4::/64, 1 successors, FD is 2816
       via Connected, GigabitEthernet0/0
P 2001:DB8:0:1::/64, 1 successors, FD is 28416
       via FE80::C820:17FF:FE04:54 (28416/2816), FastEthernet1/0
P 2001:DB8:0:14::/64, 1 successors, FD is 28160
       via Connected, FastEthernet1/0
P 2001:DB8:0:12::/64, 1 successors, FD is 28416
       via FE80::C820:17FF:FE04:54 (28416/2816), FastEthernet1/0
```

Users in the branch network of 2001:db8:0:4::/64 report that they cannot access the Internet.
Which command is issued in IPv6 router EIGRP 100 configuration mode to solve this issue?

A. Issue the eigrp stub command on R1

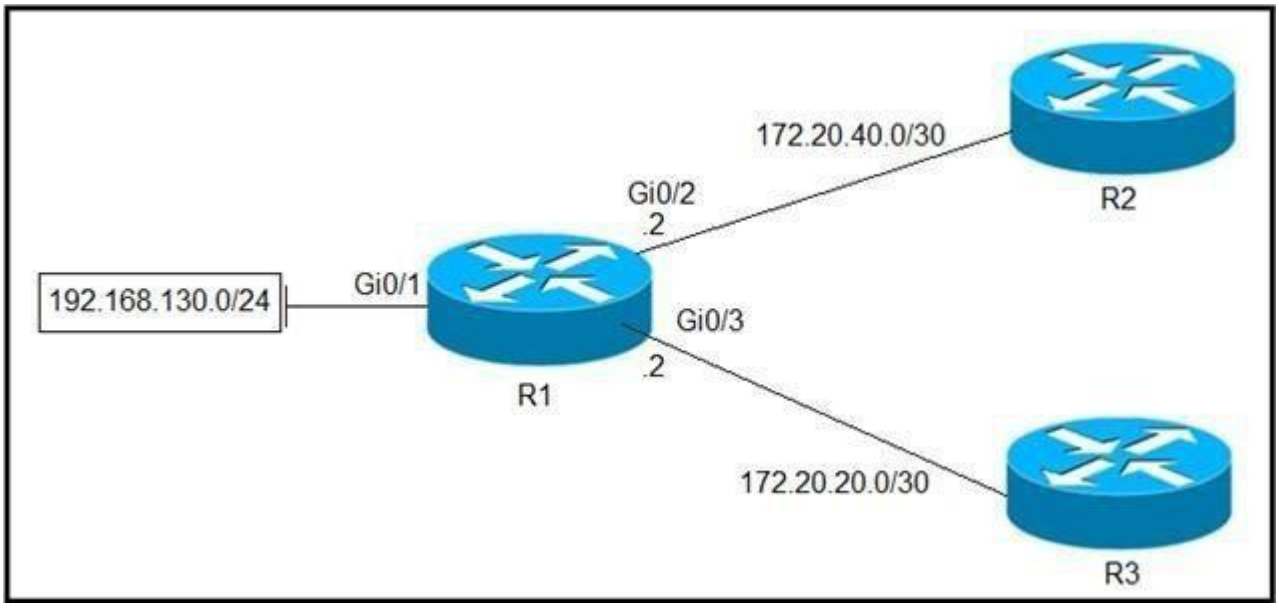
B. Issue the no neighbor stub command on R2.

C. Issue the eigrp command on R2.

D. Issue the no eigrp stub command on R1.

Answer: D

2.Refer to the exhibit.



Which configuration configures a policy on R1 to forward any traffic that is sourced from the 192.168.130.0/24 network to R2?

A.
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/2
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.20.2
```

B.
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/1
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.40.2
```

C.
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/2
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.20.1
```

D.
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/1
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.40.1
```

A. Option A
B. Option B
C. Option C
D. Option D
Answer: D

3.R2 has a locally originated prefix 192.168.130.0/24 and has these configurations:

```
ip prefix-list test seq 5 permit 192.168.130.0/24
!
route-map OUT permit10
match ip address prefix-list test
set as-path prepend 65000
```

What is the result when the route-map OUT command is applied toward an eBGP neighbor R1 (1.1.1.1) by using the neighbor 1.1.1.1 route-map OUT out command?

A. R1 sees 192.168.130.0/24 as two AS hops away instead of one AS hop away.

B. R1 does not accept any routes other than 192.168.130.0/24

C. R1 does not forward traffic that is destined for 192.168.30.0/24

D. Network 192.168.130.0/24 is not allowed in the R1 table

Answer: A

4.Which method changes the forwarding decision that a router makes without first changing the routing table or influencing the IP data plane?

A. nonbroadcast multiaccess

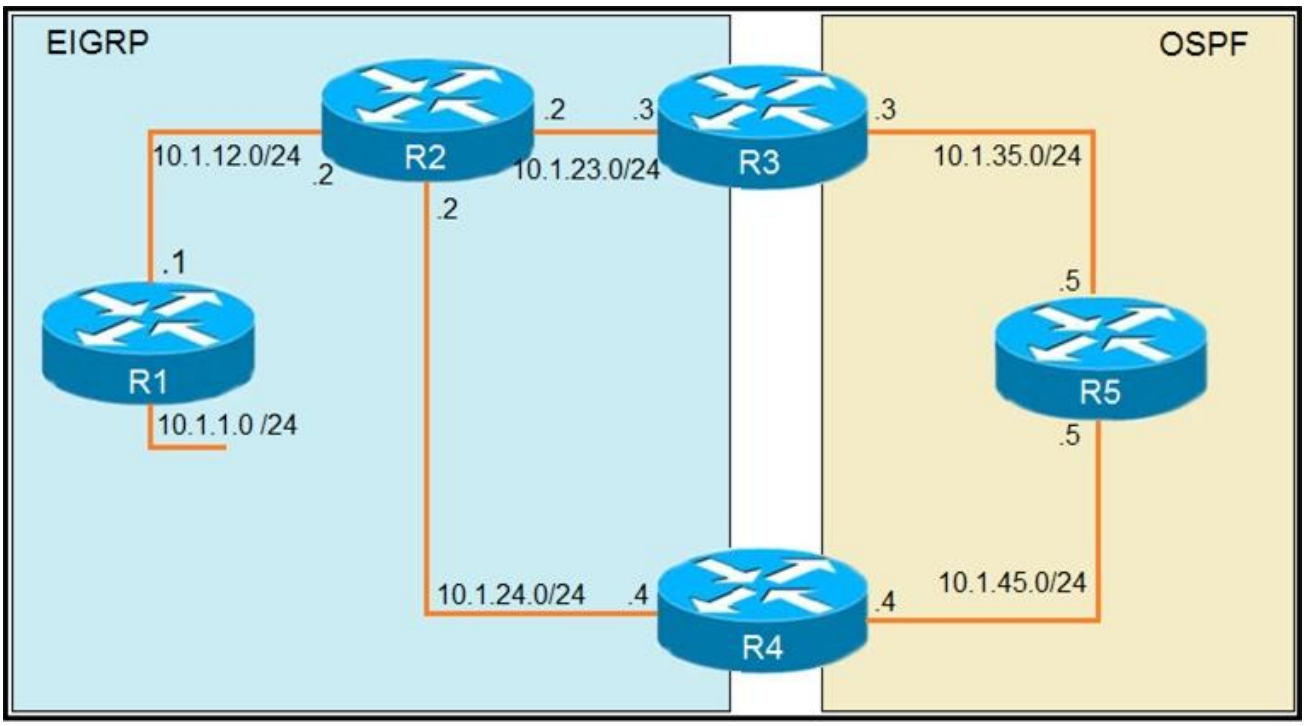
B. packet switching

C. policy-based routing

D. forwarding information base

Answer: C

5.Refer to the exhibit.



```
R1
router eigrp 1
 redistribute connected
 network 10.1.12.1 0.0.0.0

R3
router ospf 1
 redistribute eigrp 1 subnets
 network 10.1.35.3 0.0.0.0 area 0

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500
!
router ospf 1
 network 10.1.45.4 0.0.0.0 area 0

R5#traceroute 10.1.1.1

Type escape sequence to abort.
Tracing the route to 10.1.1.1

 1 10.1.35.3 80 msec 44 msec 20 msec
 2 10.1.23.2 44 msec 104 msec 64 msec
 3 10.1.24.4 44 msec 64 msec 40 msec
 4 10.1.45.5 24 msec 40 msec 20 msec
 5 10.1.35.3 92 msec 144 msec 148 msec
 6 10.1.23.2 108 msec 76 msec 80 msec
        <output truncuated>
```

The output of the trace route from R5 shows a loop in the network.

Which configuration prevents this loop?

A)

Option A

```
R3
router ospf 1
redistribute eigrp 1 subnets route-map SET-
TAG
!
route-map SET-TAG permit 10
set tag 1

R4
router eigrp 1
redistribute ospf 1 metric 2000000 1 255 1
1500 route-map FILTER-TAG
!
route-map FILTER-TAG deny 10
match tag 1
!
route-map FILTER-TAG permit 20
```

B)

Option B

```
R3
router eigrp 1
redistribute ospf 1 subnets route-map SET-
TAG
!
route-map SET-TAG permit 10
set tag 1

R4
router eigrp 1
redistribute ospf 1 metric 2000000 1 255 1
1500 route-map FILTER-TAG
network 10.1.24.4 0.0.0.0
!
route-map FILTER-TAG deny 10
match tag 1
!
route-map FILTER-TAG permit 20
```

C)

Option C

```
R3
router ospf 1
redistribute eigrp 1 subnets route-map SET-
TAG
!
route-map SET-TAG permit 10
set tag 1

R4
router eigrp 1
redistribute ospf 1 metric 2000000 1 255 1
1500 route-map FILTER-TAG
!
route-map FILTER-TAG permit 10
match tag 1
```

D)

Option D

```
R3
router ospf 1
redistribute eigrp 1 subnets route-map SET-
TAG
!
route-map SET-TAG deny 10
set tag 1

R4
router eigrp 1
redistribute ospf 1 metric 2000000 1 255 1
1500 route-map FILTER-TAG
!
route-map FILTER-TAG deny 10
match tag 1
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

Explanation:

The reason for the loop is that R2 is forwarding the packets destined to 10.1.1.1 to R4, instead of R1. This is because in the redistribute OSPF statement, BW metric has a higher value and delay has a value of 1. So, R2 chooses R4 over R1 for 10.1.1.0/24 subnet causing a loop. Now, R5 learns 10.1.1.0/24 from R3 and advertises the same route to R4, that R4 redistributes back in EIGRP. If R3 sets a tag of 1 while redistributing EIGRP in OSPF, and R4 denies all the OSPF routes with tag 1 while redistributing, it will not advertise 10.1.1.0/24 back into EIGRP. Hence, the loop will be broken.

6.Refer to the exhibit.

```
Router#show running-config | include ip route
ip route 192.168.2.2 255.255.255.255 209.165.200.225 130
Router#show ip route

<output omitted>

Gateway of last resort is not set

      192.168.1.0/32 is subnetted, 1 subnets
C           192.168.1.1 is directly connected, Loopback0
      192.168.2.0/32 is subnetted, 1 subnets
O           192.168.2.2[110/11] via 192.168.12.2, 00:52:09, Ethernet0/0
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C           192.168.12.0/24 is directly connected, Ethernet0/0
L           192.168.12.1/32 is directly connected, Ethernet0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C           209.165.200.0/24 is directly connected, Ethernet0/1
            209.165.200.226/32 is directly connected, Ethernet0/1
```

An engineer configures a static route on a router, but when the engineer checks the route to the destination, a different next hop is chosen.

What is the reason for this?

A. Dynamic routing protocols always have priority over static routes.

B. The metric of the OSPF route is lower than the metric of the static route.

C. The configured AD for the static route is higher than the AD of OSPF.

D. The syntax of the static route is not valid, so the route is not considered.

Answer: C

Explanation:

The AD of static route is manually configured to 130 which is higher than the AD of OSPF router which is 110.

7.Refer to the exhibit.

```
Router#show ip route
<output omitted>
Gateway of last resort is not set

      192.168.1.0/32 is subnetted, 1 subnets
O        192.168.1.1 [110/11] via 192.168.12.1, 16:56:40, Ethernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Loopback0
L        192.168.2.2/32 is directly connected, Loopback0
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, Ethernet0/1
L        192.168.3.1/32 is directly connected, Ethernet0/1
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, Ethernet0/0
L        192.168.12.2/32 is directly connected, Ethernet0/0
Router#show running-config | section ospf
router ospf 1
 summary-address 10.0.0.0 255.0.0.0
 redistribute static subnets
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.255 area 0
Router#
```

An engineer is trying to generate a summary route in OSPF for network 10.0.0.0/8, but the summary route does not show up in the routing table.

Why is the summary route missing?

A. The summary-address command is used only for summarizing prefixes between areas.

B. The summary route is visible only in the OSPF database, not in the routing table.

C. There is no route for a subnet inside 10.0.0.0/8, so the summary route is not generated.

D. The summary route is not visible on this router, but it is visible on other OSPF routers in the same area.

Answer: C

Explanation:

The —summary-address‖ is only used to create aggregate addresses for OSPF at an autonomous system boundary. It means this command should only be used on the ASBR when you are trying to summarize externally redistributed routes from another protocol domain or you have a NSSA area.

But a requirement to create a summarized route is:

—The ASBR compares the summary route's range of addresses with all routes redistributed into OSPF on that ASBR to find any subordinate subnets (subnets that sit inside the summary route range). If at least one subordinate subnet exists, the ASBR advertises the summary route.

8.Refer to the exhibit.

```
Router#show access-lists
Standard IP access list 1
        10 permit 192.168.2.2 (1 match)
Router#
Router#show route-map
route-map RM-OSPF-DL, permit, sequence 10
  Match clauses:
        ip address (access-lists): 1
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
Router#
Router#show running-config | section ospf
router ospf 1
  network 192.168.1.1 0.0.0.0 area 0
  network 192.168.12.0 0.0.0.255 area 0
  distribute-list route-map RM-OSPF-DL in
Router#|
```

An engineer is trying to block the route to 192.168.2.2 from the routing table by using the configuration that is shown. The route is still present in the routing table as an OSPF route.
Which action blocks the route?
A. Use an extended access list instead of a standard access list.
B. Change sequence 10 in the route-map command from permit to deny.
C. Use a prefix list instead of an access list in the route map.
D. Add this statement to the route map: route-map RM-OSPF-DL deny 20.
Answer: B

9.What is a prerequisite for configuring BFD?
A. Jumbo frame support must be configured on the router that is using BFD.
B. All routers in the path between two BFD endpoints must have BFD enabled.
C. Cisco Express Forwarding must be enabled on all participating BFD endpoints.
D. To use BFD with BGP, the timers 3 9 command must first be configured in the BGP routing process.
Answer: C
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fs_bfd.html#wp1043332

10.DRAG DROP
Drag and drop the OSPF adjacency states from the left onto the correct descriptions on the right.

Init	Each router compares the DBD packets that were received from the other router.
2-way	Routers exchange information with other routers in the multiaccess network.
Down	The neighboring router requests the other routers to send missing entries.
Exchange	The network has already elected a DR and a backup BDR.
ExStart	The OSPF router ID of the receiving router was not contained in the hello message.
Loading	No hellos have been received from a neighbor router.

Answer:

Init	Exchange
2-way	2-way
Down	Loading
Exchange	ExStart
ExStart	Init
Loading	Down

Explanation:

Reference:

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0e.shtml)

https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html

Down

This is the first OSPF neighbor state. It means that no information (hellos) has been received from this neighbor, but hello packets can still be sent to the neighbor in this state.

During the fully adjacent neighbor state, if a router doesn't receive hello packet from a neighbor within the Router Dead Interval time (RouterDeadInterval = 4*HelloInterval by default) or if the manually configured neighbor is being removed from the configuration, then the neighbor state changes from Full to Down.

Attempt

This state is only valid for manually configured neighbors in an NBMA environment. In Attempt state, the router sends unicast hello packets every poll interval to the neighbor, from which hellos have not been received within the dead interval.

Init

This state specifies that the router has received a hello packet from its neighbor, but the receiving router's ID was not included in the hello packet. When a router receives a hello packet from a neighbor, it should list the sender's router ID in its hello packet as an acknowledgment that it received a valid hello packet.

2-Way

This state designates that bi-directional communication has been established between two routers. Bi-directional means that each router has seen the other's hello packet. This state is attained when the router receiving the hello packet sees its own Router ID within the received hello packet's neighbor field. At this state, a router decides whether to become adjacent with this neighbor. On broadcast media and non-broadcast multiaccess networks, a router
becomes full only with the designated router (DR) and the backup designated router (BDR); it stays in the 2-way state with all other neighbors. On Point-to-point and Point-to-multipoint networks, a router becomes full with all connected routers.

At the end of this stage, the DR and BDR for broadcast and non-broadcast multiaccess networks are elected. For more information on the DR election process, refer to DR Election.

Note: Receiving a Database Descriptor (DBD) packet from a neighbor in the init state will also a cause a transition to 2-way state.

Exstart

Once the DR and BDR are elected, the actual process of exchanging link state information can start between the routers and their DR and BDR. (ie. Shared or NBMA networks).

In this state, the routers and their DR and BDR establish a master-slave relationship and choose the initial sequence number for adjacency formation. The router with the higher router ID becomes the master and starts the exchange, and as such, is the only router that can increment the sequence number. Note that one would logically conclude that the DR/BDR with the highest router ID will become the master during this process of master-slave relation. Remember that the DR/BDR election might be purely by virtue of a higher priority configured on the router instead of highest router ID. Thus, it is possible that a DR plays the role of slave. And also note that master/slave election is on a per-neighbor basis.

Exchange

In the exchange state, OSPF routers exchange database descriptor (DBD) packets. Database descriptors contain link-state advertisement (LSA) headers only and describe the contents of the entire link-state database. Each DBD packet has a sequence number which can be incremented only by master which is explicitly acknowledged by slave. Routers also send link-state request packets and link-state update packets (which contain the entire LSA) in this state. The contents of the DBD received are compared to the information contained in the routers link-state database to check if new or more current

link-state information is available with the neighbor.
Loading
In this state, the actual exchange of link state information occurs. Based on the information provided by the DBDs, routers send link-state request packets. The neighbor then provides the requested link-state information in link-state update packets. During the adjacency, if a router receives an outdated or missing LSA, it requests that LSA by sending a link-state request packet. All link-state update packets are acknowledged.
Full
In this state, routers are fully adjacent with each other. All the router and network LSAs are exchanged and the routers' databases are fully synchronized.
Full is the normal state for an OSPF router. If a router is stuck in another state, it is an indication that there are problems in forming adjacencies. The only exception to this is the 2-way state, which is normal in a broadcast network. Routers achieve the FULL state with their DR and BDR in NBMA/broadcast media and FULL state with every neighbor in the remaining media such as point-to-point and point-to-multipoint.
Note: The DR and BDR that achieve FULL state with every router on the segment will display FULL/DROTHER when you enter the show ip ospf neighbor command on either a DR or BDR. This simply means that the neighbor is not a DR or BDR, but since the router on which the command was entered is either a DR or BDR, this shows the neighbor as FULL/DROTHER.
Reference:
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0e.sht ml)
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html

11.Refer to the exhibit.

```
R1 #show ip bgp summary
BGP router identifier 192.168.1.1, local AS number 65000
<output omitted>
Neighbor        V  AS     MsgRcvd  MsgSent   Tblver  InQ  OutQ  Up/Down   State/PfxRcd
192.168.2.2     4  65000      28       28       22    0     0    00:21:31             0
R1#show ip bgp
BGP table version is 22, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i – internal,
              r RIB-failure, s stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, C RIB-compressed,
Origin codes: i – IGP, e – EGP, ? – incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf      Weight      Path
*>   172.16.25.0/24   209.165.200.225          0                32768       ?
R1#
```

```
R2 #show ip bgp summary
BGP router identifier 192.168.2.2, local AS number 65000
<output omitted>
Neighbor        V  AS     MsgRcvd  MsgSent   Tblver  InQ  OutQ  Up/Down   State/PfxRcd
192.168.1.1     4  65000      29       28        3    0     0    00:22:07             1
192.168.3.3     4  65000       7        8        3    0     0    00:02:55             0
R2#show ip bgp
BGP table version is 3, local router ID is 192.168.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i – internal,
              r RIB-failure, s stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, C RIB-compressed,
Origin codes: i – IGP, e – EGP, ? – incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf      Weight      Path
* i  172.16.25.0/24    209.165.200.225          0    100          0       ?
R2#
```

```
R3 #show ip bgp summary
BGP router identifier 192.168.3.3, local AS number 65000
BGP table version is 4, main routing table version 4
Neighbor        V  AS     MsgRcvd  MsgSent   Tblver  InQ  OutQ  Up/Down   State/PfxRcd
192.168.2.2     4  65000       8        7        4    0     0    00:03:08             0
R3#
```

R2 is a route reflector, and R1 and R3 are route reflector clients. The route reflector learns the route to 172.16.25.0/24 from R1, but it does not advertise to R3.

What is the reason the route is not advertised?

A. R2 does not have a route to the next hop, so R2 does not advertise the prefix to other clients.

B. Route reflector setup requires full IBGP mesh between the routers.

C. In route reflector setup, only classful prefixes are advertised to other clients.

D. In route reflector setups, prefixes are not advertised from one client to another.

Answer: A

12.Refer to the exhibit.

```
Router#sh ip route ospf
<output omitted>
Gateway is last resort is not set

      10.0.0.0/24 is subnetted, 1 subnets
   o  E2     10.0.0.0 [110/20] via 192.168.12.2, 00:00:10, Ethernet0/0
   o       192.168.3.0/24 [110/20] via 192.168.12.2, 00:00:50, Ethernet0/0
Router#

Router#show ip bgp
<output omitted>
      Network          Next Hop      Metric     LocPrf     Weight     Path
>*    192.168.1.1/32   0.0.0.0            0                32768      ?
>*    192.168.3.0      192.168.12.2      20                32768      ?
>*    192.168.12.0     0.0.0.0            0                32768      ?
Router#show running-config | section router bgp
router bgp 65000
 bgp log-neighbor-changes
 redistribute ospf 1
Router#
```

An engineer is trying to redistribute OSPF to BGP, but not all of the routes are redistributed.
What is the reason for this issue?
A. By default, only internal routes and external type 1 routes are redistributed into BGP
B. Only classful networks are redistributed from OSPF to BGP
C. BGP convergence is slow, so the route will eventually be present in the BGP table
D. By default, only internal OSPF routes are redistributed into BGP
Answer: D
Explanation:
If you configure the redistribution of OSPF into BGP without keywords, only OSPF intra-area and inter-area routes are redistributed into BGP, by default.
You can redistribute both internal and external (type-1 & type-2) OSPF routes via this command:
Router(config-router)#redistribute ospf 1 match internal external 1 external 2
Reference: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/5242-bgp-ospf-redis.html

13.Refer to the exhibit.

```
R200#show ip bgp summary
BGP router identifier 10.1.1.1, local AS number 65000
BGP table version is 26, main routing table version 26
1 network entries using 132 bytes of memory
1 path entries using 52 bytes of memory
2/1 BGP path/bestpath attribute entries using 296 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 28 bytes of memory
BGP using 508 total bytes of memory
BGP activity 24/23 prefixes, 24/23 paths, scan interval 60 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.0.2.2       4 65100   20335   20329        0    0    0 00:02:04 Idle (PfxCt)
R200#
```

In which circumstance does the BGP neighbor remain in the idle condition?

A. if prefixes are not received from the BGP peer

B. if prefixes reach the maximum limit

C. if a prefix list is applied on the inbound direction

D. if prefixes exceed the maximum limit

Answer: D

Explanation:

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/25160-bgp-maximum-prefix.html#b

14.Which attribute eliminates LFAs that belong to protected paths in situations where links in a network are connected through a common fiber?

A. shared risk link group-disjoint

B. linecard-disjoint

C. lowest-repair-path-metric

D. interface-disjoint

Answer: A

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-3s/asr1000/ire-xe-3s-asr1000/ire-ipfrr.html

15.Refer to the exhibit.

```
* Jun 28 14:41:57: %BGP-5-ADJCHANGE: neighbor 192.168.2.2 Down User reset
* Jun 28 14:41:57: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.2.2 IPv4 Unicast
topology base removed from session  User reset
* Jun 28 14:41:57: %BGP-5-ADJCHANGE: neighbor 192.168.2.2 Up
R1#show clock
*15:42:00.506 CET Fri Jun 28 2019
```

An engineer is troubleshooting BGP on a device but discovers that the clock on the device does not

correspond to the time stamp of the log entries.
Which action ensures consistency between the two times?
A. Configure the service timestamps log uptime command in global configuration mode.
B. Configure the logging clock synchronize command in global configuration mode.
C. Configure the service timestamps log datetime localtime command in global configuration mode.
D. Make sure that the clock on the device is synchronized with an NTP server.
Answer: C
Explanation:
https://www.cisco.com/c/en/us/td/docs/routers/xr12000/software/xr12k_r3-9/system_management/command/reference/yr39xr12k_chapter4.html#wp1784026936
By default, syslog and debug messages are stamped by UTC, regardless of the time zone that device configured. You should append localtime key word to "service timestamp {log | debug} datetime msec" global command to change that behavior.
https://community.cisco.com/t5/networking-documents/router-log-timestamp-entries-are-different-from-the-system-clock/ta-p/3132258
https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/cmdrefs/service_timestamps.htm

16.Refer to the exhibit.

```
R1#show policy-map control-plane
 Control Plane
        Service-policy input: CoPP-BGP
          Class-map: BGP (match all)
            2716 packets, 172071 bytes
            5 minute offered rate 0000 bps, drop rate 0000 bps
            Match: access-group name BGP
            drop

          Class-map: class-default (match-any)
            5212 packets, 655966 bytes
            5 minute offered rate 0000 bps, drop rate 0000 bps
            Match: any
```

What is the result of applying this configuration?
A. The router can form BGP neighborships with any other device.
B. The router cannot form BGP neighborships with any other device.
C. The router cannot form BGP neighborships with any device that is matched by the access list named “BGP”.
D. The router can form BGP neighborships with any device that is matched by the access list named “BGP”.
Answer: C
Explanation:
after bgp session are UP.I configured the CoPP to drop 10.3.3.3 bgp traffic (R3).

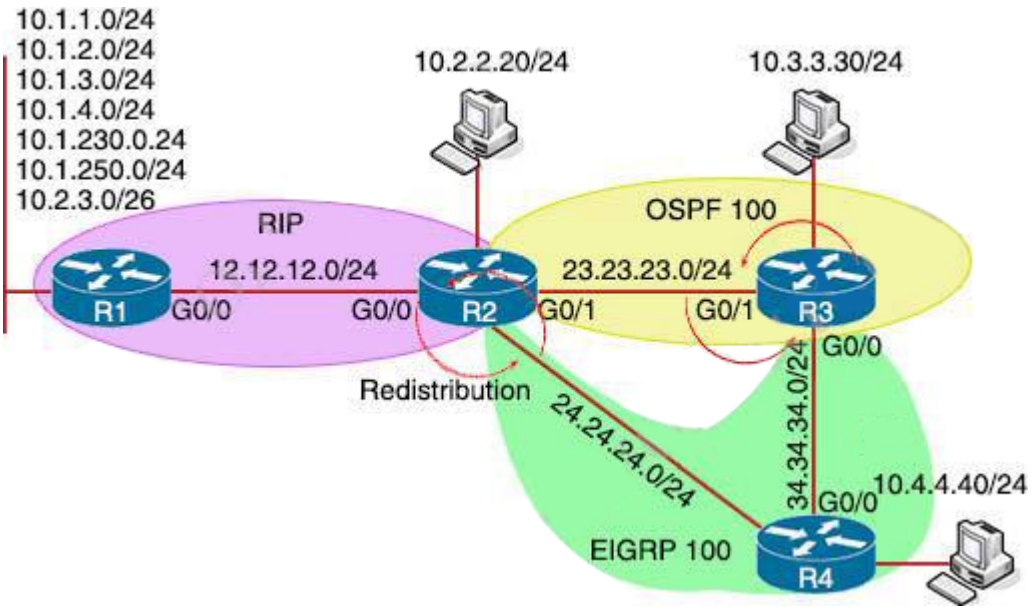
R3 bgp traffic that matched the ACL 100 is dropped and the state is in IDLE

---

access-list 100 permit tcp host 10.3.3.3 any eq bgp
access-list 100 permit tcp host 10.3.3.3 eq bgp any
!
class-map match-all class-bgp
match access-group 100
!
policy-map policy-bgp
class class-bgp
drop
!
control-plane
service-policy input policy-bgp
!
The 10.3.3.3 neighbor goes to IDLE

17.Which command displays the IP routing table information that is associated with VRF-Lite?
A. show ip vrf
B. show ip route vrf
C. show run vrf
D. show ip protocols vrf
Answer: B
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/50sg/configuration/guide/Wrapper-46SG/vrf.html#wp1045708

18.Refer to the exhibit.



```
R3
router ospf 100
 redistribute eigrp 100 subnets route-map OSPF-TAG-1

ip prefix-list OSPF-TAG-PRF seq 5 deny 10.1.0.0/16 le 24
!
ip prefix-list OSPF-TAG-PRF-1 seq 5 permit 10.2.0.0/18 le 24
!
route-map OSPF-TAG-1 deny 5
 match ip address prefix-list OSPF-TAG-PRF
 set tag 40
!
route-map OSPF-TAG-1 permit 10
 match ip address prefix-list OSPF-TAG-PRF-1
 set tag 80
!
```

Which subnet is redistributed from EIGRP to OSPF routing protocols?

A. 10.2.2.0/24

B. 10.1.4.0/26

C. 10.1.2.0/24

D. 10.2.3.0/26

Answer: A

19.Which configuration adds an IPv4 interface to an OSPFv3 process in OSPFv3 address family configuration?

A. Router ospf3 1 address-family ipv4

B. Router(config-router)#ospfv3 1 ipv4 area 0

C. Router(config-if)#ospfv3 1 ipv4 area 0

D. Router ospfv3 1 address-family ipv4 unicast

Answer: C

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-3s/iro-xe-3s-book/ip6-route-ospfv3-add-fam-xe.html

20.Refer to the exhibit.

```
R1(config)#route-map ADD permit 20
R1(config-route-map)#set tag 1

R1(config)#router ospf1
R1(config-router)#redistribute rip subnets route-map ADD
```

Which statement about R1 is true?

A. OSPF redistributes RIP routes only if they have a tag of one.

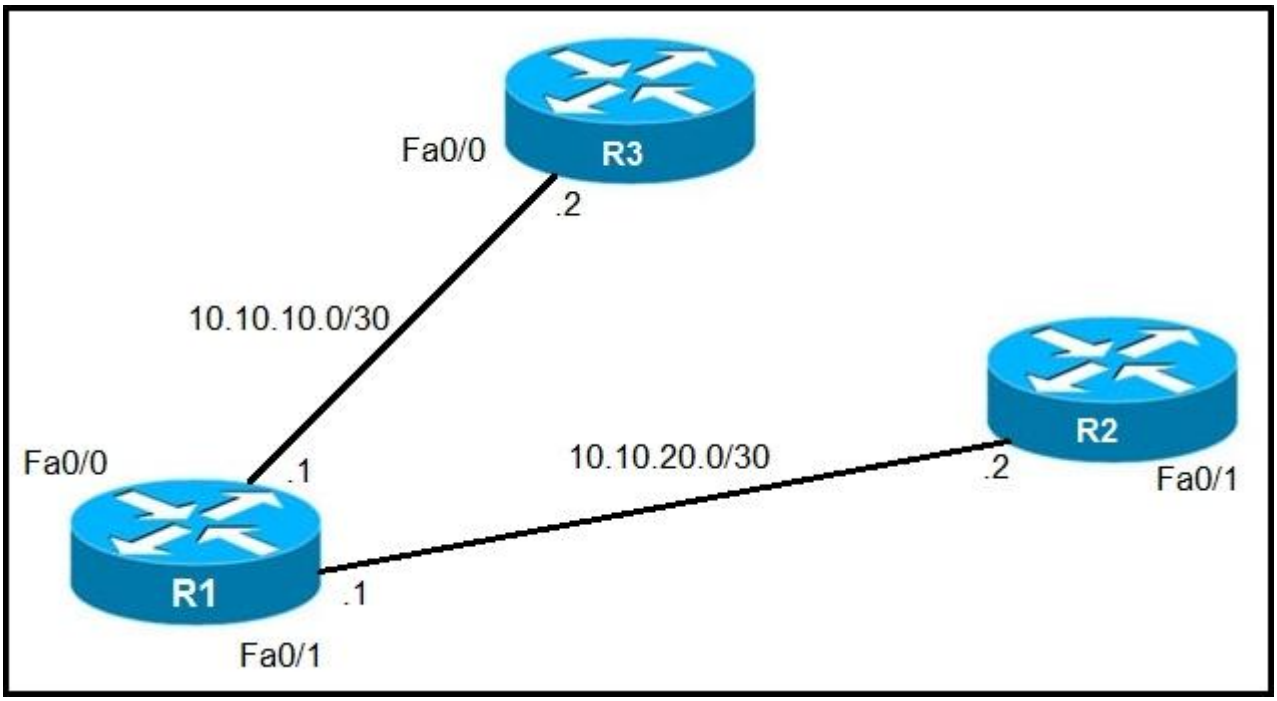
B. RIP learned routes are distributed to OSPF with a tag value of one.

C. R1 adds one to the metric for RIP learned routes before redistributing to OSPF.

D. RIP routes are redistributed to OSPF without any changes.

Answer: B

21.Refer to the exhibit.



An IP SLA was configured on router R1 that allows the default route to be modified in the event that Fa0/0 loses reachability with the router R3 Fa0/0 interface. The route has changed to flow through router R2.

Which debug command is used to troubleshoot this issue?

A. debug ip flow

B. debug ip sla error

C. debug ip routing

D. debug ip packet

Answer: C

Explanation:

debug ip routing This command enables debugging messages related to the routing table.

22.Which configuration enabled the VRF that is labeled “Inet” on FastEthernet0/0?

A. R1(config)# ip vrf Inet
R1(config-vrf)#interface FastEthernet0/0
R1(config-if)#ip vrf forwarding Inet

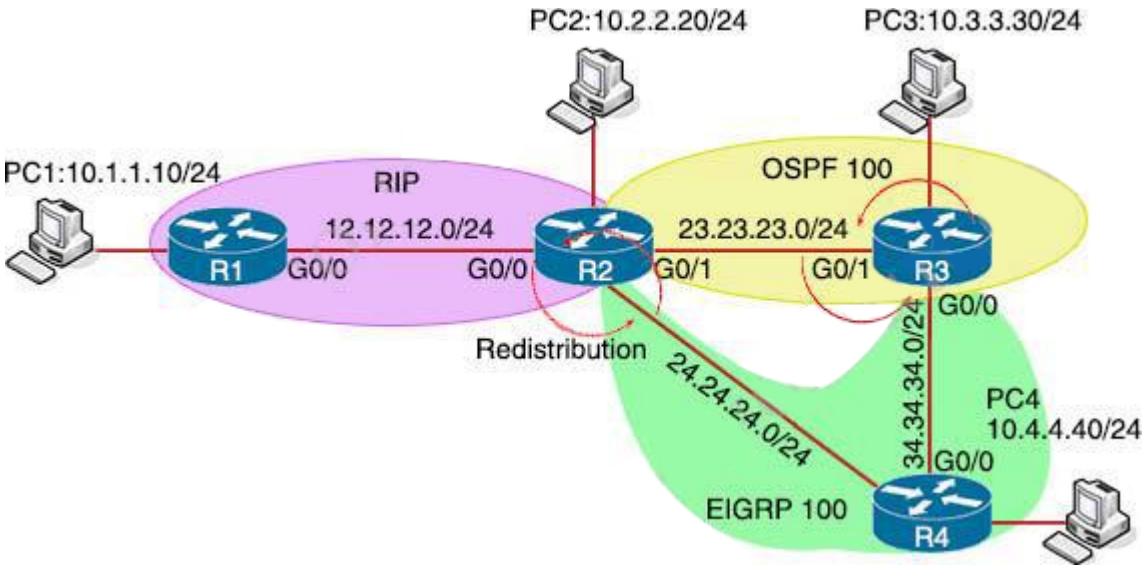
B. R1(config)#router ospf 1 vrf Inet
R1(config-router)#ip vrf forwarding FastEthernet0/0

C. R1(config)#ip vrf Inet FastEthernet0/0

D. R1(config)# ip vrf Inet
R1(config-vrf)#ip vrf FastEthernet0/0

Answer: A

23.Refer to the exhibit.



After redistribution is enabled between the routing protocols; PC2, PC3, and PC4 cannot reach PC1. Which action can the engineer take to solve the issue so that all the PCs are reachable?

A. Set the administrative distance 100 under the RIP process on R2.

B. Filter the prefix 10.1.1.0/24 when redistributed from OSPF to EIGRP.

C. Filter the prefix 10.1.1.0/24 when redistributed from RIP to EIGRP.

D. Redistribute the directly connected interfaces on R2.

Answer: A

24.Which command allows traffic to load-balance in an MPLS Layer 3 VPN configuration?

A. multi-paths eibgp 2

B. maximum-paths 2

C. Maximum-paths ibgp 2

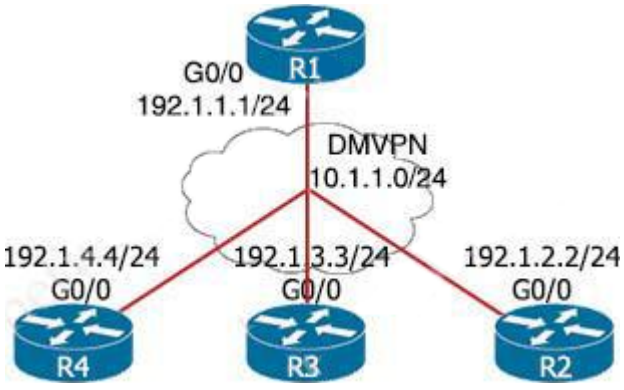
D. multi-paths 2

Answer: C

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/mpls/configuration/guide/mpls_cg/mp_vpn_multipath.html

25.Refer to the exhibit.



R2:
```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#hash md5
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2
R2(config-isakmp)#encryption 3des
R2(config)#crypto isakmp key cisco address
10.1.1.1
R2(config)#crypto ipsec transform-set TSET
esp-des esp-md5-hmac
R2(cfg-crypto-trans)#mode transport
R2(config)#crypto ipsec profile TST
R2(ipsec-profile)#set transform-set TSET
R2(config)#interface tunnel 123
E2(config-if)#tunnel protection ipsec profile
TST
```

R3:
```
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#hash md5
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 2
R3(config-isakmp)#encryption 3des
R3(config)#crypto isakmp key cisco address
10.1.1.1
R3(config)#crypto ipsec transform-set TSET
esp-des esp-md5-hmac
R3(cfg-crypto-trans)#mode tunnel
R3(config)#crypto ipsec profile TST
R3(ipsec-profile)#set transform-set TSET
R3(config)#interface tunnel 123
R3(config-if)#tunnel protection ipsec profile
TST
```

After applying IPsec, the engineer observed that the DMVPN tunnel went down, and both spoke-to-spoke and hub were not establishing.

Which two actions resolve the issue? (Choose two.)

A. Configure the crypto isakmp key cisco address 192.1.1.1 on R2 and R3

B. Configure the crypto isakmp key cisco address 0.0.0.0 on R2 and R3.

C. Change the mode from mode tunnel to mode transport on R3

D. Change the mode from mode transport to mode tunnel on R2.

E. Remove the crypto isakmp key cisco address 10.1.1.1 on R2 and R3

Answer: AD

Explanation:

*When using DMVPN with IPSec, it is unnecessary to use tunnel mode. Because DMVPN uses GRE which means that a new IP header is already added by GRE. The GRE encapsulation happens on the tunnel interface before the encryption process takes place.

26.Which statement about route distinguishers in an MPLS network is true?

A. Route distinguishers allow multiple instances of a routing table to coexist within the edge router.

B. Route distinguishers are used for label bindings.

C. Route distinguishers make a unique VPNv4 address across the MPLS network.

D. Route distinguishers define which prefixes are imported and exported on the edge router.

Answer: C

27.Which statement about MPLS LDP router ID is true?

A. If not configured, the operational physical interface is chosen as the router ID even if a loopback is configured.

B. The loopback with the highest IP address is selected as the router ID.

C. The MPLS LDP router ID must match the IGP router ID.

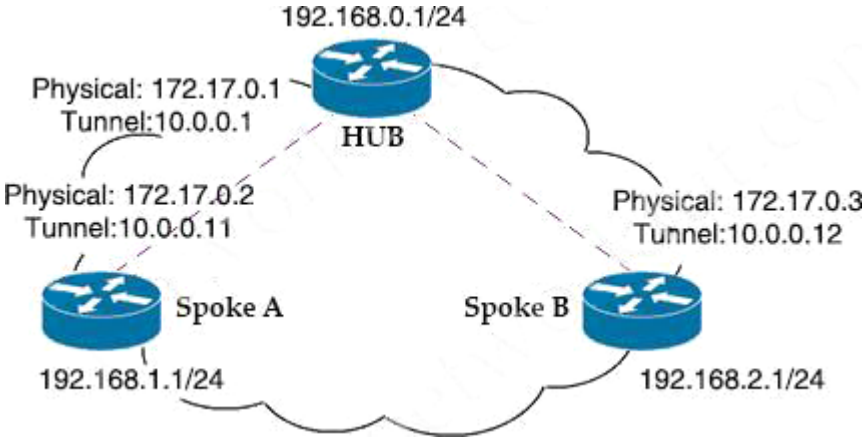
D. The force keyword changes the router ID to the specified address without causing any impact.

Answer: B

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/12-4m/mp-ldp-12-4mbook.pdf

28.Refer to the exhibit.



Which interface configuration must be configured on the spoke A router to enable a dynamic DMVPN tunnel with the spoke B router?

A.
```
interface Tunnel0
description mGRE – DMVPN Tunnel
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel destination FastEthernet 0/0
tunnel mode gre multipoint
```

B.
```
interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp network-id 1
tunnel source FastEthernet 0/0
tunnel mode gre multipoint
ip nhrp nhs 10.0.0.1
ip nhrp map 10.0.0.1 172.17.0.1
```

C.
```
interface Tunnel0
ip address 10.1.0.11 255.255.255.0
ip nhrp network-id 1
tunnel source 1.1.1.10
ip nhrp map 10.0.0.11 172.17.0.2
tunnel mode gre
```

D.
```
interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast static
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel mode gre multipoint
```

A. Option A
B. Option B
C. Option C
D. Option D
Answer: B

29.Which list defines the contents of an MPLS label?
A. 20-bit label; 3-bit traffic class; 1-bit bottom stack; 8-bit TTL
B. 32-bit label; 3-bit traffic class; 1-bit bottom stack; 8-bit TTL
C. 20-bit label; 3-bit flow label; 1-bit bottom stack; 8-bit hop limit
D. 32-bit label; 3-bit flow label; 1-bit bottom stack; 8-bit hop limit
Answer: A
Explanation:
The first 20 bits constitute a label, which can have 2^20 values. Next comes 3 bit value called Traffic Class. It was formerly called as experimental (EXP) field. Now it has been renamed to Traffic Class (TC). This field is used for QoS related functions. Ingress router can classify the packet according to some criterion and assign a 3 bit value to this filed. If an incoming packet is marked with some IP Precedence or DSCP value and the ingress router may use such a field to assign an FEC to the packet. Next bit is Stack bit which is called bottom-of-stack bit. This field is used when more than one label is assigned to a packet, as in the case of MPLS VPNs or MPLS TE. Next byte is MPLS TTL field which serves the same purpose as that of IP TTL byte in the IP header
Reference: https://tools.ietf.org/html/rfc5462

30.Refer to the exhibit.

```
Router# show tag-switching tdp bindings
(…)
tib entry: 10.10.10.1/32, rev 31
        local binding: tag: 18
        remote binding: tsr: 10.10.10.1:0, tag: imp-null
        remote binding: tsr: 10.10.10.2:0, tag: 18
        remote binding: tsr: 10.10.10.6:0, tag: 21
tib entry: 10.10.10.2/32, rev 22
        local binding: tag: 17
        remote binding: tsr: 10.10.10.2:0, tag: imp-null
        remote binding: tsr: 10.10.10.1:0, tag: 19
        remote binding: tsr: 10.10.10.6:0, tag: 22
```

What does the imp-null tag represent in the MPLS VPN cloud?

A. Pop the label

B. Impose the label

C. Include the EXP bit

D. Exclude the EXP bit

Answer: A

Explanation:

The —imp-nullǁ (implicit null) tag instructs the upstream router to pop the tag entry off the tag stack before forwarding the packet.

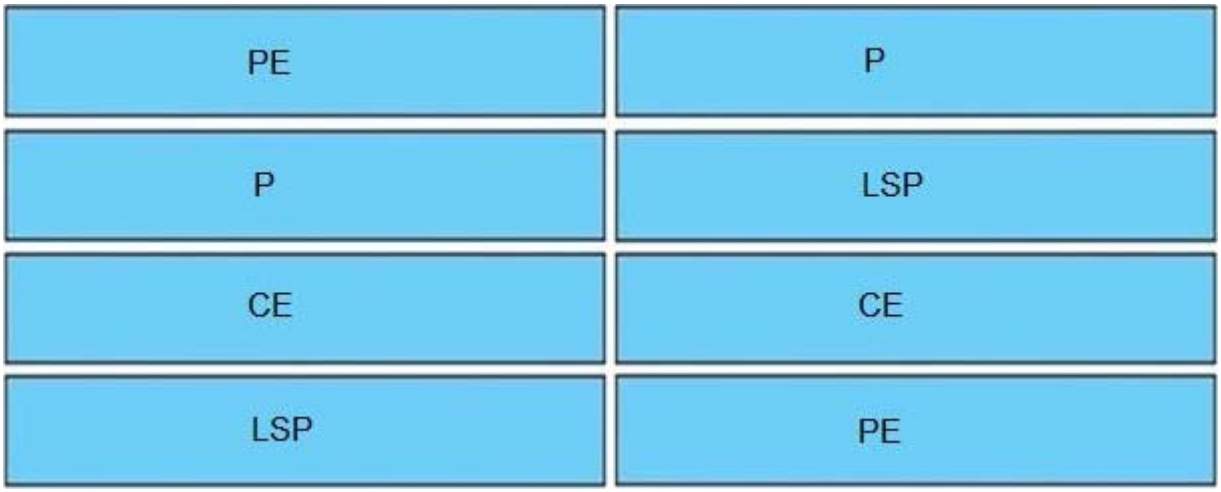
Note: pop means —remove the top MPLS labelǁ

31.DRAG DROP

Drag and drop the MPLS terms from the left onto the correct definitions on the right.

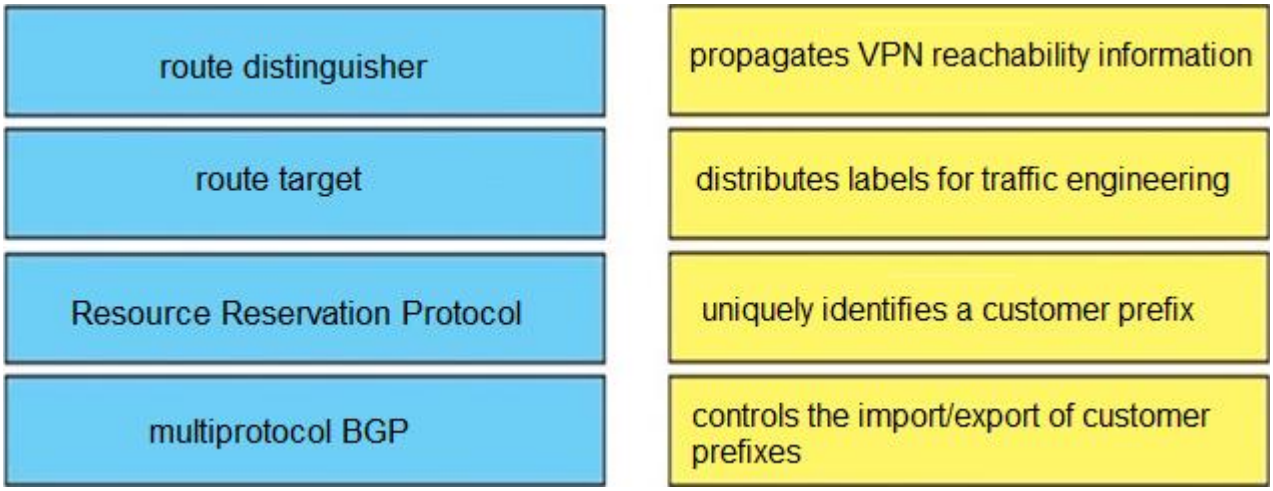
PE	device that forwards traffic based on labels
P	path that the labeled packet takes
CE	device that is unaware of MPLS labeling
LSP	device that removes and adds the MPLS labeling

Answer:



32.Which transport layer protocol is used to form LDP sessions?
A. UDP
B. SCTP
C. TCP
D. RDP
Answer: C
Explanation:
LDP multicasts hello messages to a well-known UDP port (646) in order to discover neighbors. Once the discovery is accomplished, a TCP connection (port 646) is established and the LDP session begins. LDP keepalives ensure the health of the session. Thanks to the LDP session, LDP messages create the label mappings required for a FEC. Withdraw messages are used when FECs need to be torn down.

33.DRAG DROP
Drag and drop the MPLS VPN concepts from the left onto the correct descriptions on the right.



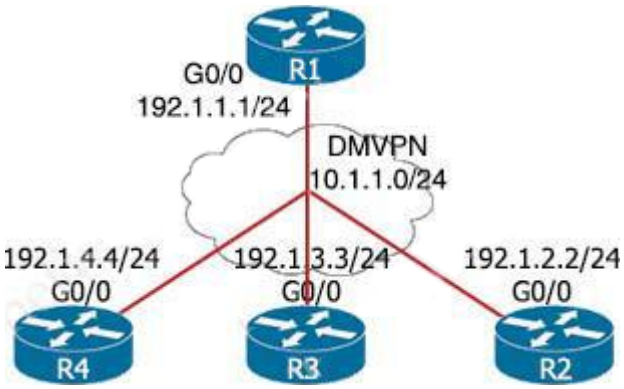
Answer:

route distinguisher	multiprotocol BGP
route target	Resource Reservation Protocol
Resource Reservation Protocol	route distinguisher
multiprotocol BGP	route target

Explanation:

Reference: https://www.rogerperkin.co.uk/featured/route-distinguisher-vs-route-target/

34.Refer to the exhibits.



On R2:

```
R2(config)#interface tunnel 1
R2(config-if)#ip address
10.1.1.2 255.255 255.0
R2(config-if)#tunnel source
FasEthernet0/0
R2(config-if)#tunnel mode gre
multipoint
R2(config-if)#ip nhrp network-
id 222
R2(config-if)#ip nhrp nhs
10.1.1.1
R2(config-if)#ip nhrp map
10.1.1.1 192.1.1.1
```

On R3:

```
R3(config)#interface tunnel 1
R3(config-if)#ip address
10.1.1.3 255.255.255.0
R3(config-if)#tunnel source
FastEthernet0/0
R3(config-if)#tunnel mode gre
multipoint
R3(config-if)#ip nhrp network-
id 333
R3(config-if)#ip nhrp nhs
10.1.1.1
R3(config-if)#ip nhrp map
10.1.1.1 192.1.1.1
```

On R4:

```
R4(config)#interface tunnel 1
R4(config-if)#ip address
10.1.1.4 255.255.255 0
R4(config-ff)#tunnel source
FastEthernet0/0
R4(config-if)#tunnel mode gre
multipoint
R4(config-if)#ip nhrp network-
id 444
R4(config-if)#ip nhrp nhs
10.1.1.1
R4(config-if)#ip nhrp map
10.1.1.1 192.1.1.1
```

Phase-3 tunnels cannot be established between spoke-to-spoke in DMVPN.

Which two commands are missing? (Choose two.)

A. The ip nhrp redirect command is missing on the spoke routers.

B. The ip nhrp shortcut command is missing on the spoke routers.

C. The ip nhrp redirect commands is missing on the hub router.

D. The ip nhrp shortcut commands is missing on the hub router.
E. The ip nhrp map command is missing on the hub router.
Answer: BC

35.Which protocol is used to determine the NBMA address on the other end of a tunnel when mGRE is used?
A. NHRP
B. IPsec
C. MP-BGP
D. OSPF
Answer: A

36.Refer to the exhibit.

Which configuration denies Telnet traffic to router 2 from 198A:0:200C::1/64?
A)

```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64 eq telnet
!
int Gi0/0
 ipv6 traffic-filter Deny_Telnet in
!
```

B)

```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64 eq telnet
!
int Gi0/0
 ipv6 access-map Deny_Telnet in
!
```

C)

```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64
!
int Gi0/0
 ipv6 access-map Deny_Telnet in
!
```

D)

```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64
!
int Gi0/0
 ipv6 traffic-filter Deny_Telnet in
!
```

A. Option A
B. Option B
C. Option C
D. Option D
Answer: A

37.Refer to the exhibit.

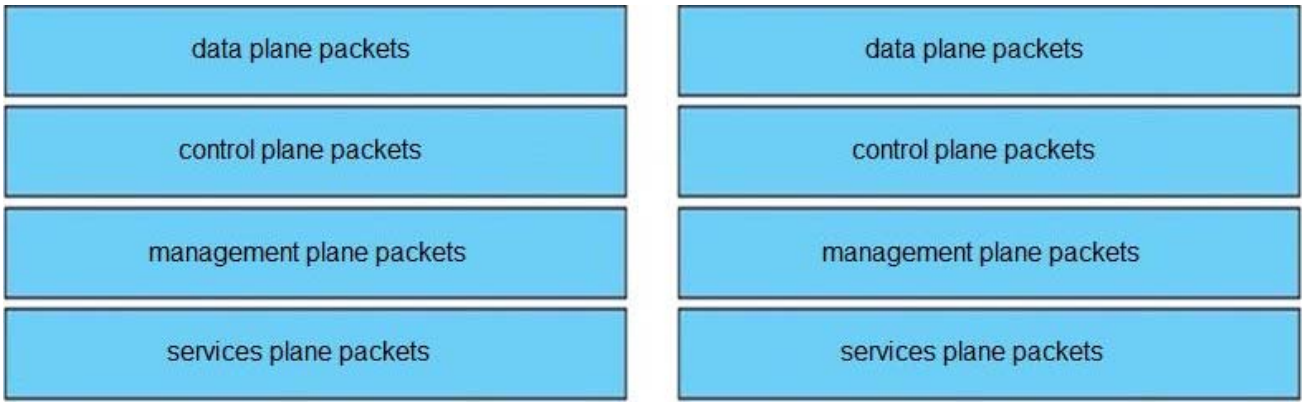
```
access-list 100 deny tcp any any eq 465
access-list 100 deny tcp any eq 465 any
access-list 100 permit tcp any any eq 80
access-list 100 permit tcp any eq 80 any
access-list 100 permit udp any any eq 443
access-list 100 permit udp any eq 443 any
```

During troubleshooting it was discovered that the device is not reachable using a secure web browser.
What is needed to fix the problem?
A. permit tcp port 443
B. permit udp port 465
C. permit tcp port 465
D. permit tcp port 22
Answer: A

38.DRAG DROP
Drag and drop the packet types from the left onto the correct descriptions on the right.

data plane packets	user-generated packets that are always forwarded by network devices to other end-station devices
control plane packets	network device generated or received packets that are used for the creation of the network itself
management plane packets	network device generated or received packets; packets that are used to operate the network
services plane packets	user-generated packets that are forwarded by network devices to other end-station devices, but that require higher priority than the normal traffic by the network devices

Answer:



Explanation:

Unlike legacy network technologies such as ISDN, Frame Relay, and ATM that defined separate data and control channels, IP carries all packets within a single pipe. Thus, IP network devices such as routers and switches must be able to distinguish between data plane, control plane, and management plane packets to treat each packet appropriately.

From an IP traffic plane perspective, packets may be divided into four distinct, logical groups:

1. Data plane packets – End-station, user-generated packets that are always forwarded by network devices to other end-station devices. From the perspective of the network device, data plane packets always have a transit destination IP address and can be handled by normal, destination IP address-based forwarding processes.
2. Control plane packets – Network device generated or received packets that are used for the creation and operation of the network itself. From the perspective of the network device, control plane packets always have a receive destination IP address and are handled by the CPU in the network device route processor. Examples include protocols such as ARP, BGP, OSPF, and other protocols that glue the network together.
3. Management plane packets – Network device generated or received packets, or management station generated or received packets that are used to manage the network. From the perspective of the network device, management plane packets always have a receive destination IP address and are handled by the CPU in the network device route processor. Examples include protocols such as Telnet, Secure Shell (SSH), TFTP, SNMP, FTP, NTP, and other protocols used to manage the device and/or network.
4. Services plane packets – A special case of data plane packets, services plane packets are also user-generated packets that are also forwarded by network devices to other end-station devices, but that require high-touch handling by the network device (above and beyond normal, destination IP address-based forwarding) to forward the packet. Examples of high-touch handling include such functions as GRE encapsulation, QoS, MPLS VPNs, and SSL/IPsec encryption/decryption, etc. From the perspective of the network device, services plane packets may have a transit destination IP address, or may have a receive destination IP address (for example, in the case of a VPN tunnel endpoint).

Reference: https://tools.cisco.com/security/center/resources/copp_best_practices

39.DRAG DROP

Drag and drop the addresses from the left onto the correct IPv6 filter purposes on the right.

permit ip 2001:d8b:800:200c:: /117 2001:0DBB:800:2010::/64 eq 443	Permit NTP from this source 2001:0D8B:0800:200c::1f
permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514	Permit syslog from this source 2001:0D88:0800:200c::1c
permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80	Permit HTTP from this source 2001:0D8B:0800:200c::0fff
permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123	Permit HTTPS from this source 2001:0D8B:0800:200c::07ff

Answer:

permit ip 2001:d8b:800:200c:: /117 2001:0DBB:800:2010::/64 eq 443	permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123
permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514	permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514
permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80	permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80
permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123	permit ip 2001:d8b:800:200c:: /117 2001:0DBB:800:2010::/64 eq 443

Explanation:

HTTP and HTTPs run on TCP port 80 and 443, respectively and we have to remember them.
Syslog runs on UDP port 514 while NTP runs on UDP port 123 so if we remember them we can find out the matching answers easily. But maybe there is some typos in this question as 2001: d88:800:200c::c/126 only ranges from 2001:d88:800:200c:0:0:0:c to 2001:d88:800:200c:0:0:0:f (4 hosts in total). It does not cover host 2001:0D88:0800:200c::1f. Same for 2001:D88:800:200c::e/126, which also ranges from 2001:d88:800:200c:0:0:0:c to 2001:d88:800:200c:0:0:0:f and does not cover host 2001:0D88:0800:200c::1c.

40.Refer to the exhibit.

```
R1#show running-config | include aaa
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication login Console local
R1#show running-config | section line
line con 0
 logging synchronous
R1#
```

An engineer is trying to configure local authentication on the console line, but the device is trying to authenticate using TACACS+.
Which action produces the desired configuration?

A. Add the aaa authentication login default none command to the global configuration.
B. Replace the capital “C” with a lowercase “c” in the aaa authentication login Console local command.
C. Add the aaa authentication login default group tacacs+ local-case command to the global configuration.
D. Add the login authentication Console command to the line configuration
Answer: D
Explanation:
Reference: https://community.cisco.com/t5/switching/how-to-define-login-local-for-console-0/td-p/2949493

41.Refer to the exhibit.

```
R1#show ip ssh
SSH Disabled – version 1.99
%Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size: 1024 bits
IOS Keys in SECSH format (ssh-rsa, base64 encoded) : NONE
R1#
```

An engineer is trying to connect to a device with SSH but cannot connect. The engineer connects by using the console and finds the displayed output when troubleshooting.
Which command must be used in configuration mode to enable SSH on the device?
A. no ip ssh disable
B. ip ssh enable
C. ip ssh version 2
D. crypto key generate rsa
Answer: D

42.Which statement about IPv6 ND inspection is true?
A. It learns and secures bindings for stateless autoconfiguration addresses in Layer 3 neighbor tables.
B. It learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables.
C. It learns and secures bindings for stateful autoconfiguration addresses in Layer 3 neighbor tables.
D. It learns and secures bindings for stateful autoconfiguration addresses in Layer 2 neighbor tables.
Answer: B
Explanation:
IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables. IPv6 ND inspection analyzes neighbor discovery messages in order to build a trusted binding table database, and IPv6 neighbor discovery messages that do not have valid bindings are dropped. A neighbor discovery message is considered trustworthy if its IPv6-to-MAC mapping is verifiable.
This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-s/ip6f-15-s-book/ip6-snooping.pdf

43.While troubleshooting connectivity issues to a router, these details are noticed:
- Standard pings to all router interfaces, including loopbacks, are successful.
- Data traffic is unaffected.
- SNMP connectivity is intermittent.
- SSH is either slow or disconnects frequently.

Which command must be configured first to troubleshoot this issue?
A. show policy-map control-plane
B. show policy-map
C. show interface | inc drop
D. show ip route
Answer: A

44.Refer to the exhibit.

```
TAC+: TCP/IP open to 171.68.118.101/49 failed --
Destination unreachable; gateway or host down
AAA/AUTHEN (2546660185): status = ERROR
AAA/AUTHEN/START (2546660185): Method=LOCAL
AAA/AUTHEN (2546660185): status = FAIL
As1 CHAP: Unable to validate Response. Username chapuser: Authentication failure
```

Why is user authentication being rejected?
A. The TACACS+ server expects “user”, but the NT client sends “domain/user”.
B. The TACACS+ server refuses the user because the user is set up for CHAP.
C. The TACACS+ server is down, and the user is in the local database.
D. The TACACS+ server is down, and the user is not in the local database.
Answer: D
Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-accesscontrol-system-tacacs-/13864-tacacs-pppdebug.html

45.Refer to the exhibit.

```
Cat3850-Stack-2# show policy-map

Policy Map LIMIT_BGP
  Class BGP
    drop

Policy Map SHAPE_BGP
  Class BGP
    Average Rate Traffic Shaping
    cir 10000000 (bps)

Policy Map POLICE_BGP
  Class BGP
    police cir 1000k bc 1500
      conform-action transmit
      exceed-action transmit

Policy Map COPP
  Class BGP
    police cir 1000k bc 1500
      conform-action transmit
      exceed-action drop
```

Which control plane policy limits BGP traffic that is destined to the CPU to 1 Mbps and ignores BGP traffic that is sent at higher rate?

A. policy-map SHAPE_BGP

B. policy-map LIMIT_BGP

C. policy-map POLICE_BGP

D. policy-map COPP

Answer: D

46.Which statement about IPv6 RA Guard is true?

A. It does not offer protection in environments where IPv6 traffic is tunneled.

B. It cannot be configured on a switch port interface in the ingress direction.

C. Packets that are dropped by IPv6 RA Guard cannot be spanned.

D. It is not supported in hardware when TCAM is programmed.

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-3s/ip6f-xe-3s-book/ip6-ra-guard.html#GUID-589AF00C-7499-439F-AD23-51005D61CAB7

The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is tunneled.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16/ip6f-xe-16-book/ip6-ra-guard.pdf

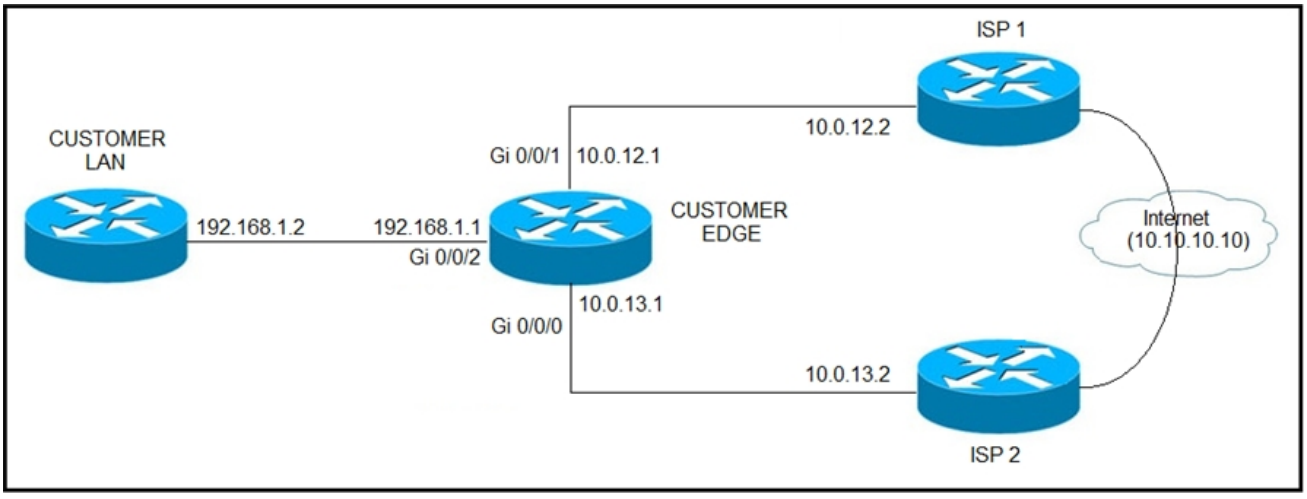
47.An engineer is trying to copy an IOS file from one router to another router by using TFTP.
Which two actions are needed to allow the file to copy? (Choose two.)
A. Copy the file to the destination router with the copy tftp: flash: command
B. Enable the TFTP server on the source router with the tftp-server flash: <filename> command
C. TFTP is not supported in recent IOS versions, so an alternative method must be used
D. Configure a user on the source router with the username tftp password tftp command
E. Configure the TFTP authentication on the source router with the tftp-server authentication local command
Answer: AB

48.Refer to the exhibit.

```
R1#show running-config | section dhcp
ip dhcp excluded-address 192.168.1.1 192.168.1.49
ip dhcp pool DHCP
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
   dns-server 8.8.8.8
   lease 0 12
```

Users report that IP addresses cannot be acquired from the DHCP server. The DHCP server is configured as shown. About 300 total nonconcurrent users are using this DHCP server, but none of them are active for more than two hours per day.
Which action fixes the issue within the current resources?
A. Modify the subnet mask to the network 192.168.1.0 255.255.254.0 command in the DHCP pool
B. Configure the DHCP lease time to a smaller value
C. Configure the DHCP lease time to a bigger value
D. Add the network 192.168.2.0 255.255.255.0 command to the DHCP pool
Answer: B

49.Refer to the exhibit.



ISP 1 and ISP 2 directly connect to the Internet. A customer is tracking both ISP links to achieve redundancy and cannot see the Cisco IOS IP SLA tracking output on the router console.
Which command is missing from the IP SLA configuration?
A. Start-time 00:00
B. Start-time 0
C. Start-time immediately
D. Start-time now
Answer: D
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book/sla_icmp_echo.html

50.Refer to the exhibit.

```
service timestamps debug datetime msec
service timestamps log datetime
clock timezone MST -7 0
clock summer-time MST recurring
ntp authentication-key 1 md5 00101A0B01521812062247470 71E 7
ntp server 10.10.10.10

R1#show clock
*06:13:44.045 MST Sun Dec 30 2018

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config) #logging host 10.10.10.20
R1(config) #end
R1#
*Dec 30 13:15:28: %SYS-5-CONFIG_I: Configured from console by console
R1#
*Dec 30 13:15:28: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.10.10.20 port 514
started – CLI initiated
```

An administrator noticed that after a change was made on R1, the timestamps on the system logs did not match the clock.
What is the reason for this error?
A. An authentication error with the NTP server results in an incorrect timestamp.
B. The keyword localtime is not defined on the timestamp service command.
C. The NTP server is in a different time zone.
D. The system clock is set incorrectly to summer-time hours.
Answer: B

51.DRAG DROP
Drag and drop the DHCP messages from the left onto the correct uses on the right.

DHCPACK	server-to-client communication, refusing the request for configuration parameters
DHCPINFORM	client-to-server communication, indicating that the network address is already in use
DHCPNAK	server-to-client communication with configuration parameters, including committed network address
DHCPDECLINE	client-to-server communication, asking for only local configuration parameters that the client has already externally configured as an address

Answer:

DHCPACK	DHCPACK
DHCPINFORM	DHCPDECLINE
DHCPNAK	DHCPNAK
DHCPDECLINE	DHCPINFORM

Explanation:

Reference: https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.html

DHCPINFORM: If a client has obtained a network address through some other means or has a manually configured IP address, a client workstation may use a DHCPINFORM request message to obtain other local configuration parameters, such as the domain name and Domain Name Servers (DNSs). DHCP servers receiving a DHCPINFORM message construct a DHCPACK message with any local configuration parameters appropriate for the client without allocating a new IP address. This DHCPACK will be sent unicast to the client.

DHCPNAK: If the selected server is unable to satisfy the DHCPREQUEST message, the DHCP server will respond with a DHCPNAK message. When the client receives a DHCPNAK message, or does not receive a response to a DHCPREQUEST message, the client restarts the configuration process by going into the Requesting state. The client will retransmit the DHCPREQUEST at least four times within 60 seconds before restarting the Initializing state.

DHCPACK: After the DHCP server receives the DHCPREQUEST, it acknowledges the request with a DHCPACK message, thus completing the initialization process.

DHCPDECLINE: The client receives the DHCPACK and will optionally perform a final check on the parameters. The client performs this procedure by sending Address Resolution Protocol (ARP) requests for the IP address provided in the DHCPACK. If the client detects that the address is already in use by

receiving a reply to the ARP request, the client will send a DHCPDECLINE message to the server and restart the configuration process by going into the Requesting state.
Reference: https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.html

52.A network engineer is investigating a flapping (up/down) interface issue on a core switch that is synchronized to an NTP server. Log output currently does not show the time of the flap.
Which command allows the logging on the switch to show the time of the flap according to the clock on the device?
A. service timestamps log uptime
B. clock summer-time mst recurring 2 Sunday mar 2:00 1 Sunday nov 2:00
C. service timestamps log datetime localtime show-timezone
D. clock calendar-valid
Answer: C
Explanation:
By default, Catalyst switches add a simple uptime timestamp to logging messages. This is a cumulative counter that shows the hours, minutes, and seconds since the switch has been booted up

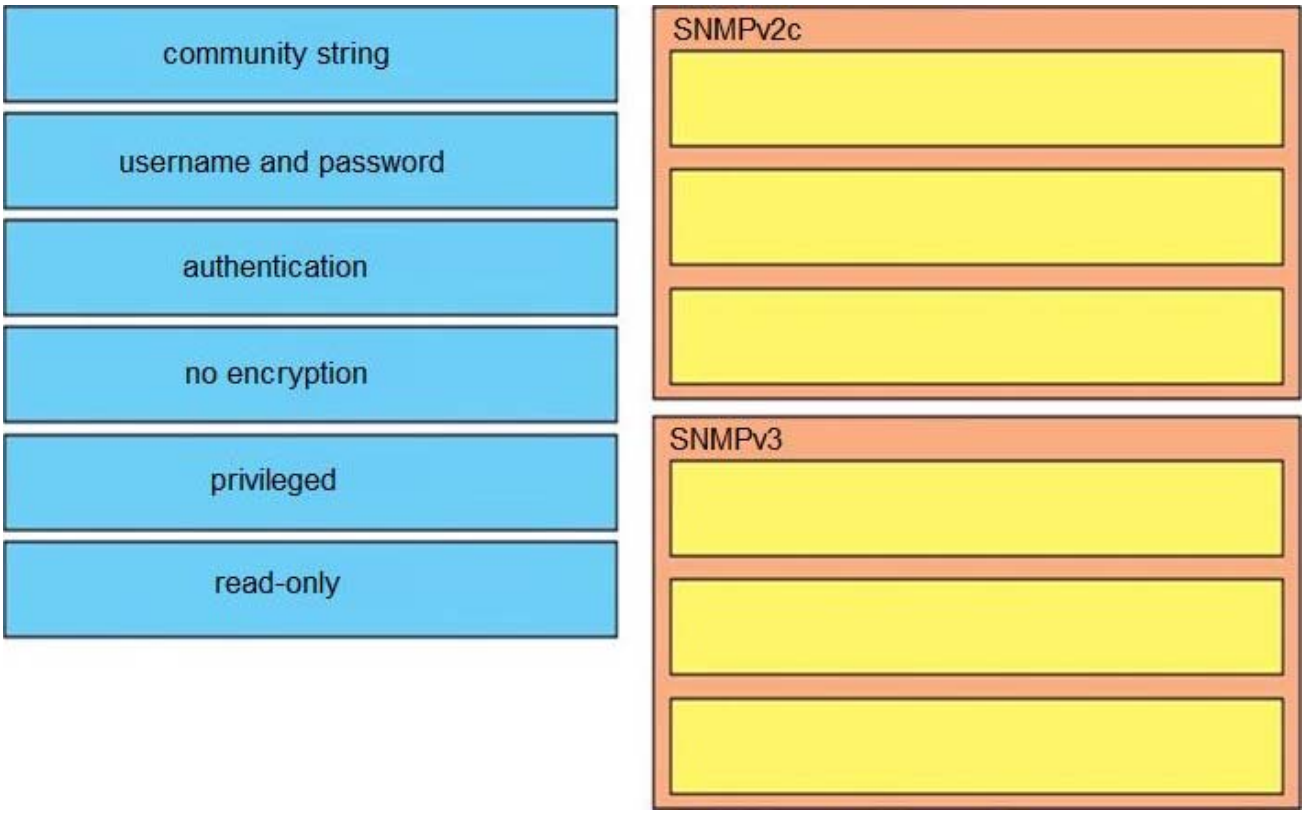
53.When provisioning a device in Cisco DNA Center, the engineer sees the error message “Cannot select the device. Not compatible with template”.
What is the reason for the error?
A. The template has an incorrect configuration.
B. The software version of the template is different from the software version of the device.
C. The changes to the template were not committed.
D. The tag that was used to filter the templates does not match the device tag.
Answer: D
Explanation:
If you use tags to filter the templates, you must apply the same tags to the device to which you want to apply the templates. Otherwise, you get the following error during provisioning:
—Cannot select the device. Not compatible with template.
Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-10/user_guide/b_cisco_dna_center_ug_1_2_10/b_dnac_ug_1_2_10_chapter_0111.html

54.While working with software images, an engineer observes that Cisco DNA Center cannot upload its software image directly from the device.
Why is the image not uploading?
A. The device must be resynced to Cisco DNA Center.
B. The software image for the device is in install mode.
C. The device has lost connectivity to Cisco DNA Center.
D. The software image for the device is in bundle mode
Answer: B
Explanation:
Upload Software Images for Devices in Install Mode

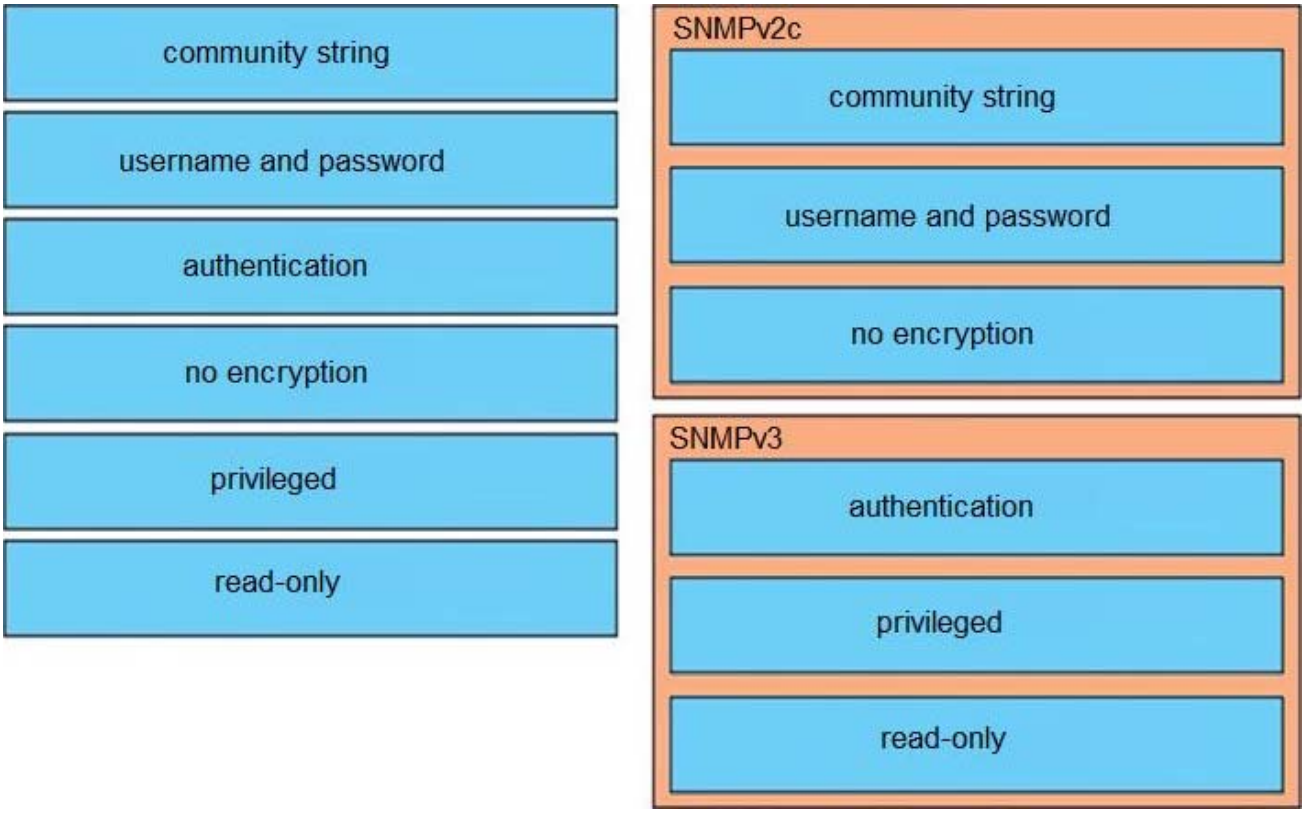
The Image Repository page might show a software image as being in Install Mode. When a device is in Install Mode, Cisco DNA Center is unable to upload its software image directly from the device. When a device is in install mode, you must first manually upload the software image to the Cisco DNA Center repository before marking the image as golden, as shown in the following steps.
Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-andmanagement/dna-center/1-2-10/user_guide/b_cisco_dna_center_ug_1_2_10/b_dnac_ug_1_2_10_chapter_0100.html

55.An engineer configured the wrong default gateway for the Cisco DNA Center enterprise interface during the install.
Which command must the engineer run to correct the configuration?
A. sudo maglev-config update
B. sudo maglev install config update
C. sudo maglev reinstall
D. sudo update config install
Answer: A

56.DRAG DROP
Drag and drop the SNMP attributes in Cisco IOS devices from the left onto the correct SNMPv2c or SNMPV3 categories on the right.



Answer:



57.Refer to the exhibit.

```
R1(config) # do show running-config | section line|username
username cisco secret 5 $1$yb/o$L3G5cXODxpYMSJ70PzEyo0
line con 0
 logging synchronous
line vty 0 4
 login local
 transport input telnet
R1(config) # logging console 7
R1(config) # do debug aaa authentication
R1(config) #
```

An administrator that is connected to the console does not see debug messages when remote users log in.
Which action ensures that debug messages are displayed for remote logins?
A. Enter the transport input ssh configuration command.
B. Enter the terminal monitor exec command.
C. Enter the logging console debugging configuration command.
D. Enter the aaa new-model configuration command.
Answer: C
Explanation:

The —logging consolell is a default and hidden command.

58.Refer to the exhibit.

```
snmp-server community ciscotest1
snmp-server host 192.168.1.128 ciscotest
snmp-sever enable traps bgp
```

Network operations cannot read or write any configuration on the device with this configuration from the operations subnet.
Which two configurations fix the issue? (Choose two.)
A. Configure SNMP rw permission in addition to community ciscotest.
B. Modify access list 1 and allow operations subnet in the access list.
C. Modify access list 1 and allow SNMP in the access list.
D. Configure SNMP rw permission in addition to version 1.
E. Configure SNMP rw permission in addition to community ciscotest 1.
Answer: B E

59.Refer to the exhibit.

```
config t
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow exporter EXPORTER-1
 destination 172.16.10.2
 transport udp 90
 exit
!
flow monitor FLOW-MONITOR-1
 record v4_r1
 exit
!
ip cef
!
interface Ethernet0/0.1
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!
```

Why is the remote NetFlow server failing to receive the NetFlow data?

A. The flow exporter is configured but is not used.

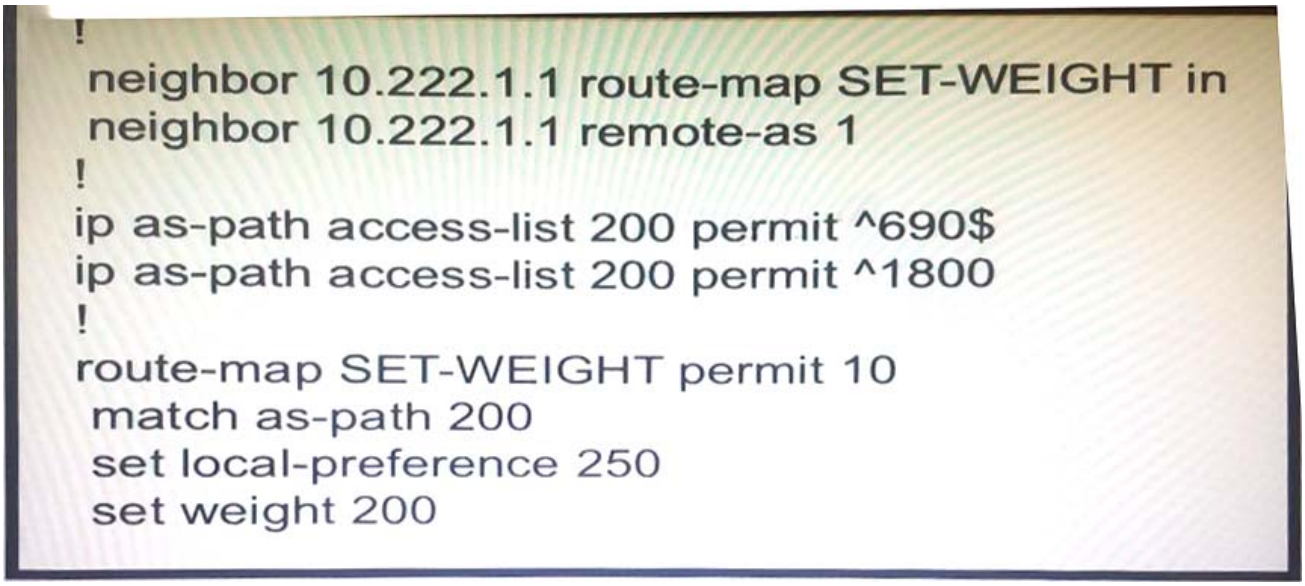
B. The flow monitor is applied in the wrong direction.

C. The flow monitor is applied to the wrong interface.

D. The destination of the flow exporter is not reachable.

Answer: A

60.Refer to the exhibit.



A router receiving BGP routing updates from multiple neighbors for routers in AS 690.
What is the reason that the router still sends traffic that is destined to AS 690 to a neighbor other than 10.222.1.1?
A. The local preference value in another neighbor statement is higher than 250.
B. The local preference value should be set to the same value as the weight in the route map.
C. The route map is applied in the wrong direction.
D. The weight value in another neighbor statement is higher than 200.
Answer: C

61.Refer to the exhibit.

```
Router#show ip route
…
D 192.168.32.0/19 [90/25789217] via 10.1.1.1
R 192.168.32.0/24 [120/4] via 10.1.1.2
O 192.168.32.0/26 [110/229840] via 10.1.1.3
```

An engineer is trying to get 192.168.32.100 forwarded through 10.1.1.1, but it was forwarded through 10.1.1.2.
What action forwards the packets through 10.1.1.1?
A. Configure EIGRP to receive 192.168.32.0 route with lower admin distance.
B. Configure EIGRP to receive 192.168.32.0 route with longer prefix than /19.
C. Configure EIGRP to receive 192.168.32.0 route with lower metric.
D. Configure EIGRP to receive 192.168.32.0 route with equal or longer prefix than /24.
Answer: D

62.What is a limitation of IPv6 RA Guard?
A. It is not supported in hardware when TCAM is programmed
B. It does not offer protection in environments where IPv6 traffic is tunneled.
C. It cannot be configured on a switch port interface in the ingress direction
D. Packets that are dropped by IPv6 RA Guard cannot be spanned

Answer: B
Explanation:
Restrictions for IPv6 RA Guard
- The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is tunneled.
- This feature is supported only in hardware when the ternary content addressable memory (TCAM) is programmed.
- This feature can be configured on a switch port interface in the ingress direction.
- This feature supports host mode and router mode.
- This feature is supported only in the ingress direction; it is not supported in the egress direction.
- This feature is not supported on EtherChannel and EtherChannel port members.
- This feature is not supported on trunk ports with merge mode.
- This feature is supported on auxiliary VLANs and private VLANs (PVLANs). In the case of PVLANs, primary VLAN features are inherited and merged with port features.
- Packets dropped by the IPv6 RA Guard feature can be spanned.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16-10/ip6f-xe-16-10-book/ip6-ra-guard.html#GUID-589AF00C-7499-439F-AD23-51005D61CAB7

63.Refer to the exhibit.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.1
R1(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.2 10
R1(config)#ip sla 1
R1(config)#icmp-echo 1.1.1.1 source-interface FastEthernet0/0
R1(config)#ip sla schedule 1 life forever start-time now
R1(config)#track 1 ip sla 1 reachability
```

An IP SLA is configured to use the backup default route when the primary is down, but it is not working as desired.
Which command fixes the issue?
A. R1(config)# ip route 0.0.0.0.0.0.0.2.2.2.2 10 track 1
B. R1(config)# ip route 0.0.0.0.0.0.0.2.2.2.2
C. R1(config)#ip sla track 1
D. R1(config)# ip route 0.0.0.0.0.0.0.1.1.1.1 track 1
Answer: D
Explanation:
Note: By default Static Router AD value-1 hence ip route 0.0.0.0. 0.0.0.0. 1.1.1.1 track 1 means AD-1 which must be less than of back up route AD.
Define the backup route to use when the tracked object is unavailable.
!--- The administrative distance of the backup route must be greater than
!--- the administrative distance of the tracked route.
!--- If the primary gateway is unreachable, that route is removed
!--- and the backup route is installed in the routing table
!--- instead of the tracked route.
https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200785-ISP-Failover-with-default-routes-using-I.html

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118962-configure-asa-00.html

64.Which label operations are performed by a label edge router?
A. SWAP and POP
B. SWAP and PUSH
C. PUSH and PHP
D. PUSH and POP
Answer: D
Explanation:
A label edge router (LER, also known as edge LSR) is a router that operates at the edge of an MPLS network and acts as the entry and exit points for the network. LERs push an MPLS label onto an incoming packet and pop it off an outgoing packet.
Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/mpls/configuration/guide/mpls_cg/mp_mpls_overview.pdf

65.Refer to the exhibit.

```
BRANCH-RTR#

router eigrp 100
 network 10.4.31.0 0.0.0.7
 network 10.100.100.1 0.0.0.0
 distribute-list route-map FILTER-IN in FastEthernet0/0
 eigrp router-id 10.100.100.1
!
ip prefix-list 102 seq 10 permit 10.1.1.100/32
!
route-map FILTER-IN deny 10
 match ip address prefix-list 102
!
```

A junior engineer updated a branch router configuration. Immediately after the change, the engineer receives calls from the help desk that branch personnel cannot reach any network destinations.
Which configuration restores service and continues to block 10.1.1.100/32?
A. route-map FILTER-IN deny 5
B. ip prefix-list 102 seq 15 permit 0.0.0.0/32 le 32
C. ip prefix-list 102 seq 5 permit 0.0.0.0/32 le 32
D. route-map FILTER-IN permit 20
Answer: D
Explanation:
By using “deny” keyword in a route-map, we can filter out the prefix specified in the prefix-list.
But there is an implicit “deny all” statement in the prefix-list so we must permit other prefixes with “permit” keyword in the route-map.

66.An engineer configured a leak-map command to summarize EIGRP routes and advertise specifically loopback 0 with an IP of 10.1.1.1.255.255.255.252 along with the summary route. After finishing

configuration, the customer complained not receiving summary route with specific loopback address.

```
router eigrp 1
!
route_map Leak-Route deny 10
!
interface Serial 0/0
ip summary-address eigrp 1 10.0.0.0 255.0.0.0 leak-map Leak-Route
```

Which two configurations will fix it? (Choose two.)

A. Configure access-list 1 permit 10.1.1.0.0.0.0.3.

B. Configure access-list 1 permit 10.1.1.1.0.0.0.252.

C. Configure access-list 1 and match under route-map Leak-Route.

D. Configure route-map Leak-Route permit 10 and match access-list 1.

E. Configure route-map Leak-Route permit 20.

Answer: AD

Explanation:

When you configure an EIGRP summary route, all networks that fall within the range of your summary are suppressed and no longer advertised on the interface. Only the summary route is advertised. But if we want to advertise a network that has been suppressed along with the summary route then we can use leak-map feature.

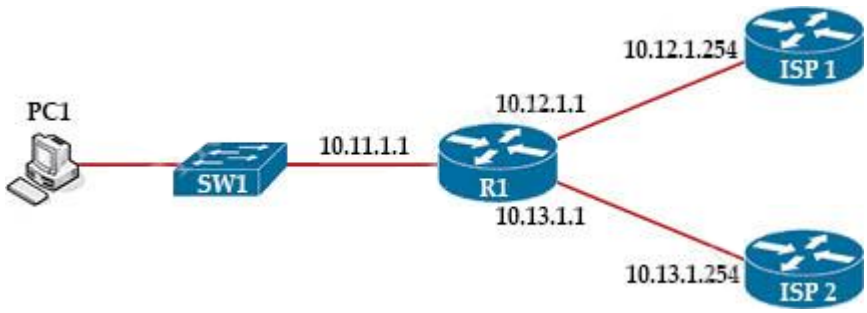
The below commands will fix the configuration in this question:

R1(config)#access-list 1 permit 10.1.1.0 0.0.0.3

R1(config)#route-map Leak-Route permit 10 // this command will also remove the “route_map Leak-Route deny 10” command.

R1(config-route-map)#match ip address 1

67.Refer to the exhibit.



```
R1
ip sla 100
 icmp-echo 10.12.1.254
!
track 10 ip sla 100 reachability
!
ip route 0.0.0.0 0.0.0.0 10.12.1.254 track 10
ip route 0.0.0.0 0.0.0.0 10.13.1.254 10
!
R1#show ip route
--Output Omitted--
Gateway of last resort is 10.13.1.254 to network 0.0.0.0

S*    0.0.0.0/0 [10/0] via 10.13.1.254
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.11.1.0/24 is directly connected, GigabitEthernet0/1
L        10.11.1.1/32 is directly connected, GigabitEthernet0/1
C        10.12.1.0/24 is directly connected, GigabitEthernet0/0
L        10.12.1.1/32 is directly connected, GigabitEthernet0/0
C        10.13.1.0/24 is directly connected, GigabitEtheraet0/2
L        10.13.1.1/32 is directly connected, GigabitEthernet0/2
```

An engineer is monitoring reachability of the configured default routes to ISP1 and ISP2. The default route from ISP1 is preferred if available.
How is this issue resolved?
A. Use the icmp-echo command to track both default routes
B. Use the same AD for both default routes
C. Start IP SLA by matching numbers for track and ip sla commands
D. Start IP SLA by defining frequency and scheduling it
Answer: D
Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200785-ISP-Failover-with-default-routes-using-I.html
In the above configuration we have not had activated our IP SLA operation.
We can start it with this command:
R1(config)#ip sla schedule 100 life forever start-time now
Also we should specific the rate of ICMP echo:
R1(config-ip-sla-echo)#frequency 5 // Send ICMP echo every 5 seconds

68.After some changes in the routing policy, it is noticed that the router in AS 45123 is being used as a transit AS router for several service provides.
Which configuration ensures that the branch router in AS 45123 advertises only the local networks to all SP neighbors?
A)

```
ip as-path access-list 1 permit  ^45123
!
router bgp 45123
 neighbor SP-Neighbors filter-list 1 out
```

B)

```
ip as-path access-list 1 permit .*
!
router bgp 45123
 neighbor SP-Neighbors filter-list 1 out
```

C)

```
ip as-path access-list 1 permit ^45123$
!
router bgp 45123
 neighbor SP-Neighbors filter-list 1 out
```

D)

```
ip as-path access-list 1 permit ^$
!
router bgp 45123
 neighbor SP-Neighbors filter-list 1 out
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

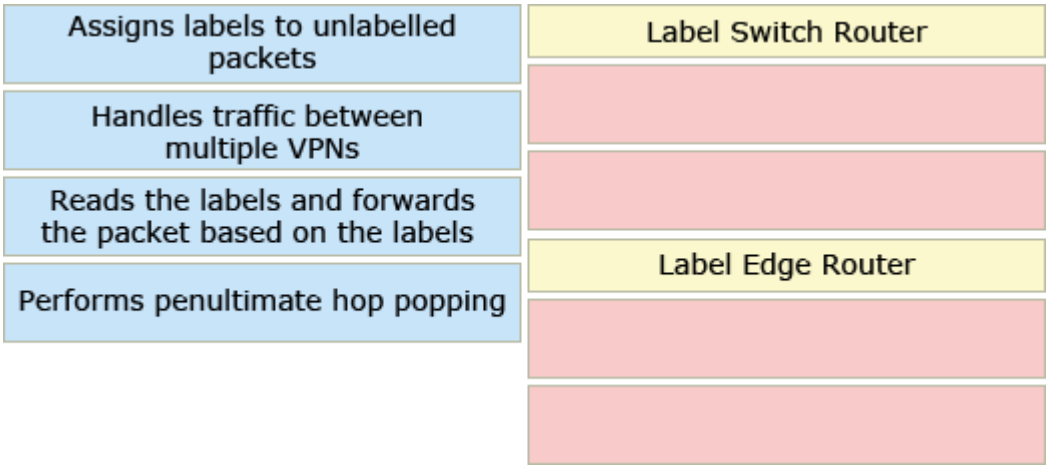
By default BGP advertises all prefixes to external BGP neighbors. This means that if you are multi-homed (connected to two or more ISPs) then you might become a transit AS. For example, ISP 2 in AS 200 can send traffic to your router in AS 100 to reach ISP 3 in AS 300 because you advertised prefixes in ISP 3 to ISP 2.

This is what will be seen in the BGP routing table of ISP1:

```
ISP1#show ip bgp
--output omitted--
 Network          Next Hop            Metric LocPrf Weight Path
....
*> 3.3.3.0/24     192.168.12.1                           0 100 300 i
```

69.DRAG DROP

Drag and drop the operations from the left onto the locations where the operations are performed on the right.



Answer:

Assigns labels to unlabelled packets	Label Switch Router
Handles traffic between multiple VPNs	Reads the labels and forwards the packet based on the labels
Reads the labels and forwards the packet based on the labels	Performs penultimate hop popping
Performs penultimate hop popping	Label Edge Router
	Assigns labels to unlabelled packets
	Handles traffic between multiple VPNs

Explanation:

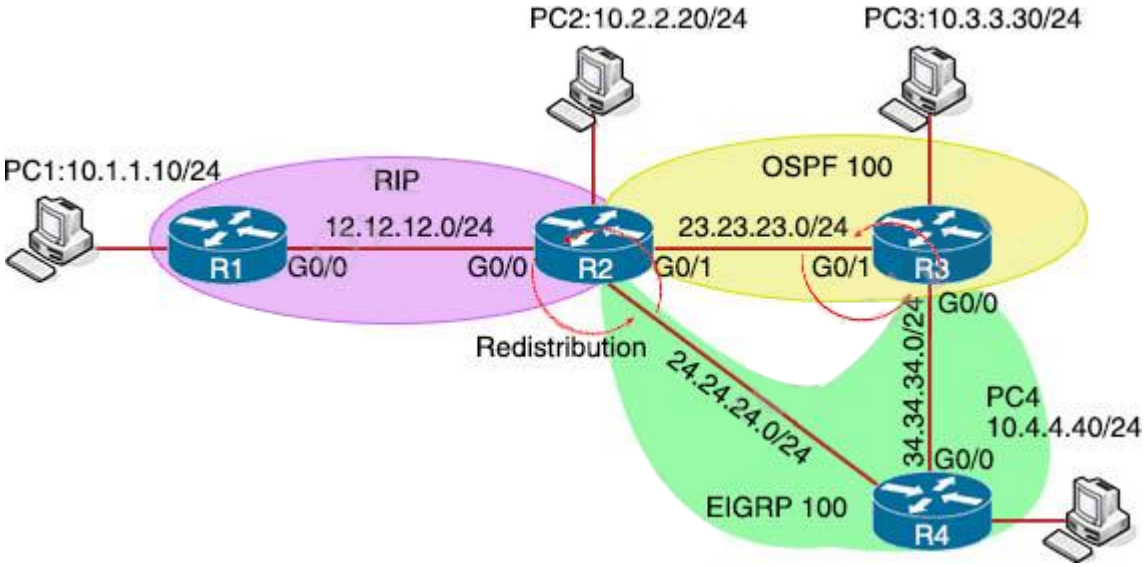
Label Switch Router

1. Reads labels and forwards the packet based on the based on the label.
2. Performs PHP

Label Edge Router:

1 Assigns labels and unlabeled packets.
2. Handles traffic between multiple VPNs

70.Refer to the exhibit.



Redistribution is enabled between the routing protocols, and nowPC2 PC3, and PC4 cannot reach PC1. What are the two solutions to fix the problem? (Choose two.)

A. Filter RIP routes back into RIP when redistributing into RIP in R2
B. Filter OSPF routes into RIP FROM EIGRP when redistributing into RIP in R2.
C. Filter all routes except RIP routes when redistributing into EIGRP in R2.
D. Filter RIP AND OSPF routes back into OSPF from EIGRP when redistributing into OSPF in R2
E. Filter all routes except EIGRP routes when redistributing into OSPF in R3.

Answer: A, C

Even PC2 cannot reach PC1 so there is something wrong with RIP redistribution in R2. Because

RIP has higher Administrative Distance (AD) value than OSPF and EIGRP so it will be looped when doing mutual redistribution.

71.Refer to the exhibit.

```
R1#show policy-map control-plane
  Control Plane
  Class-map: NMS (match-all)
  500461 packets, 24038351 bytes
  5 minute offered rate 1390000 bps, drop rate 0 bps
  police:
    cir 50000 bps, bc 5000 bytes
  conformed 50444 packets, 24031001 bytes; actions:
    transmit
  exceeded 990012 packets, 94030134 bytes; actions:
    drop
  conformed 4000 bps, exceed 0 bps
```

A company is evaluating multiple network management system tools. Trending graphs generated by SNMP data are returned by the NMS and appear to have multiple gaps. While troubleshooting the issue, an engineer noticed the relevant output.
What solves the gaps in the graphs?
A. Remove the exceed-rate command in the class map.
B. Remove the class map NMS from being part of control plane policing.
C. Configure the CIR rate to a lower value that accommodates all the NMS tools
D. Separate the NMS class map in multiple class maps based on the specific protocols with appropriate CoPP actions
Answer: D
Explanation:
Reference: https://tools.cisco.com/security/center/resources/copp_best_practices
The class-map NMS in the exhibit did not classify traffic into specific protocols so many packets were dropped. We should create some class-map to classify the receiving traffic.
It is also a recommendation of CoPP/CPP policy:
“Developing a CPP policy starts with the classification of the control plane traffic. To that end, the control plane traffic needs to be first identified and separated into different class maps.”

72.What is a role of route distinguishers in an MPLS network?
A. Route distinguishers define which prefixes are imported and exported on the edge router
B. Route distinguishers allow multiple instances of a routing table to coexist within the edge router.
C. Route distinguishers are used for label bindings.
D. Route distinguishers make a unique VPNv4 address across the MPLS network
Answer: D

73.Refer to the exhibit.

```
Global RADIUS shared secret:*******
retransmission count: 5
timeout value: 10
following RADIUS servers are configured:
 myradius.network.users.com:
   available for authentication on port: 1814
   available for accounting on port: 1813
10.1.1.1:
   available for authentication on port: 1814
   available for accounting on port: 1813
   RADIUS shared secret: ******
10.2.2.3
   available for authentication on port: 1814
   available for accounting on port: 1813
RADIUS shared secret: ******
```

AAA server 10.1.1.1 is configured with the default authentication and accounting settings, but the switch cannot communicate with the server.
Which action resolves this issue?
A. Match the authentication port
B. Match the accounting port
C. Correct the timeout value.
D. Correct the shared secret.
Answer: A
Explanation:
Command Default
Accounting port: 1813
Authentication port: 1812
Accounting: enabled
Authentication: enabled
Retransmission count: 1
Idle-time: 0
Server monitoring: disabled
Timeout: 5 seconds
Test username: test
Test password: test
Reference: https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/radius-server-host.html
By default, RADIUS uses UDP port 1812 for authentication and port 1813 for accounting. In the exhibit above we see port 1814 is being used for authentication to AAA server at 10.1.1.1 which is not the default port so we must adjust the authentication port to the default value 1812.

74.DRAG DROP

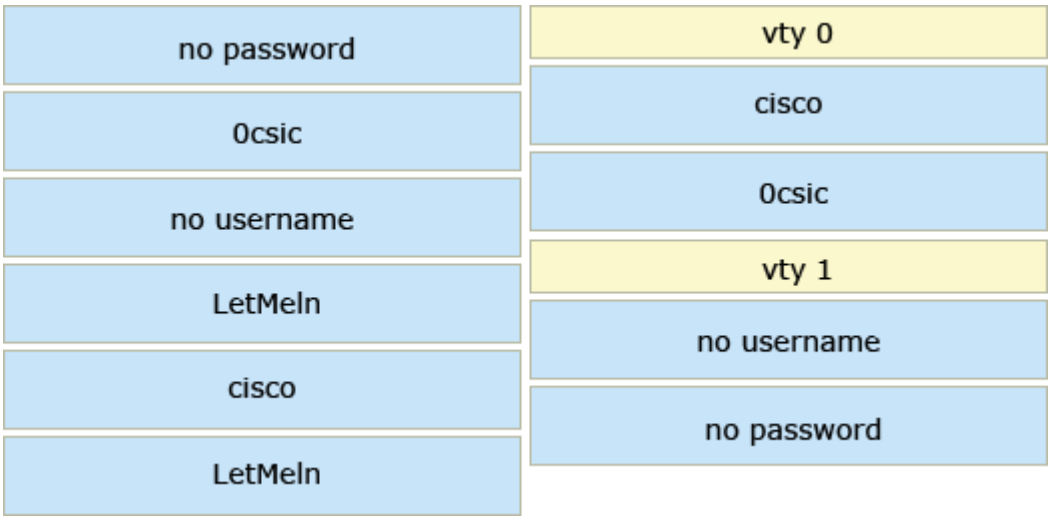
Refer to the exhibit.

```
aaa new-model
aaa authentication login default none
aaa authentication login telnet local
!
username cisco password 0 ocsic
!
line vty 0
 password LetMeIn
 login authentication telnet
 transport input telnet
line vty 1
 password LetMeIn
 transport input telnet
```

Drag and drop the credentials from the left onto the remote login information on the right to resolve a failed login attempt to vtys. Not all credentials are uf SLA by defining frequency and schedulingsed

no password	vty 0
0csic	username
no username	password
LetMeIn	vty 1
cisco	username
LetMeIn	password

Answer:



Explanation:
vty 0:
+ cisco
+ 0csic
vty 1:
+ no username
+ no password
The command “aaa authentication login default none” means no authentication is required when access to the device via Console/VTY/AUX so if one interface does not specify another login authentication method (via the “login authentication …” command), it will allow to access without requiring username or password. In this case VTY 1 does not specify another authentication login method so it will use the default method (which is “none” in this case).

75.Refer to the exhibit.

The network administrator configured VRF lite for customer A. The technician at the remote site misconfigured VRF on the router.

Which configuration will resolve connectivity for both sites of customer_a?

- ip vrf customer_a
  rd 1:1
  route-target export 1:2
  route-target import 1:2

- ip vrf customer_a
  rd 1:1
  route-target import 1:1
  route-target export 1:2

- ip vrf customer_a
  rd 1:2
  route-target both 1:2

- ip vrf customer_a
  rd 1:2
  route-target both 1:1

A. Option A

B. Option B

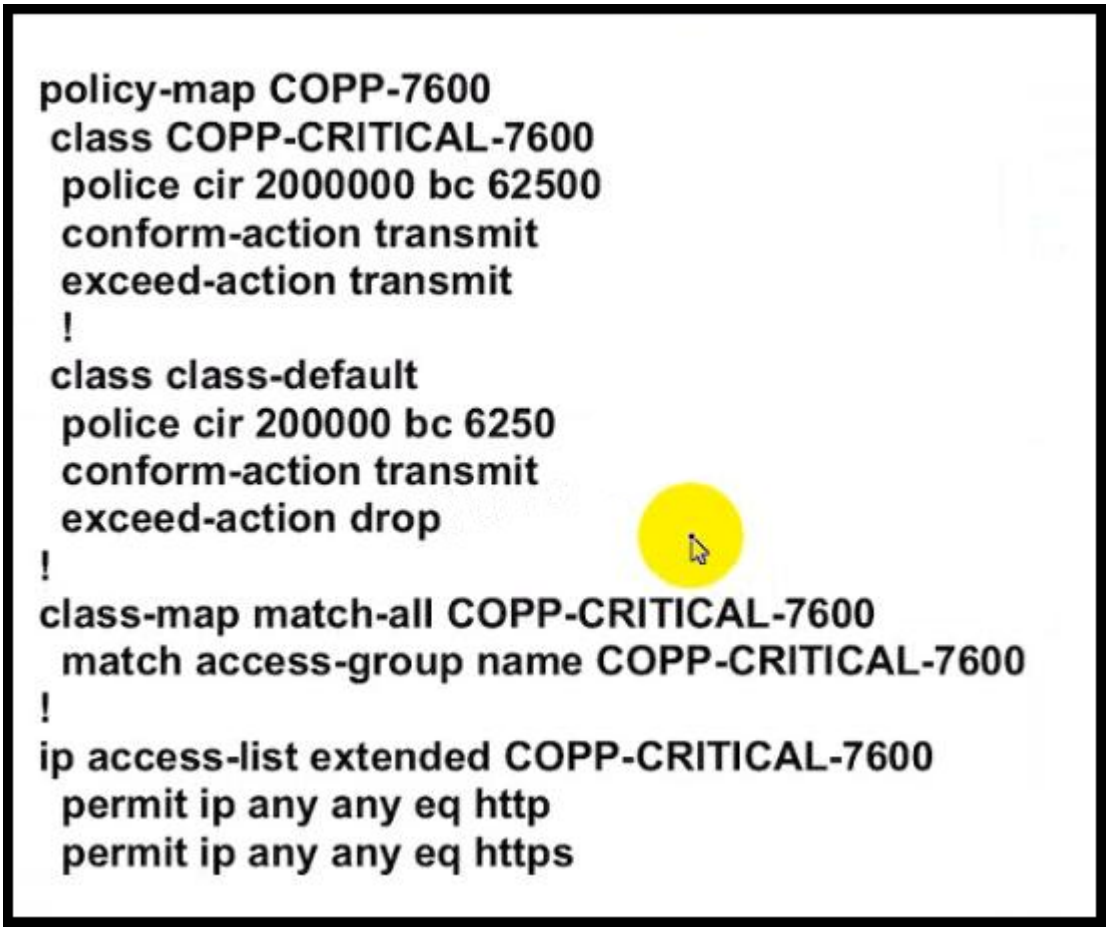
C. Option C

D. Option D

Answer: D
Explanation:
From the exhibit, we learned:
+ VRF customer_a was exported with Route target (RT) of 1:1 so at the remote site it must be imported with the same RT 1:1.
+ VRF customer_a was imported with Route target (RT) of 1:1 so at the remote site it must be exported with the same RT 1:1.
Therefore at the remote site we must configure the command “route-target both 1:1” (which is equivalent to two commands “route-target import 1:1” & “route-target export 1:1”.

76.What is a function of IPv6 ND inspection?
A. It learns and secures bindings for stateless autoconfiguration addresses in Layer 3 neighbor tables
B. It learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables
C. It learns and secures bindings for stateful autoconfiguration addresses in Layer 2 neighbor tables.
D. It learns and secures bindings for stateful autoconfiguration addresses in Layer 3 neighbor tables.
Answer: B

77.Exhibit:



BGP is flapping after the Copp policy is applied.
What are the two solutions to fix the issue? (Choose two)
A. Configure BGP in the COPP-CRITICAL-7600 ACL

B. Configure a higher value for CIR under the default class to allow more packets during peak traffic
C. Configure a higher value for CIR under the class COPP-CRITICAL-7600
D. Configure a three-color policer instead of two-color policer under class COPP-CRITICAL-7600
E. Configure IP CEF to CoPP policy and BGP to work
Answer: AB
Explanation:
The policy-map COPP-7600 only rate-limit HTTP & HTTPS traffic (based on the ACL conditions) so any BGP packets will be processed in the class “class-default”, which drops exceeded BGP packets.
Therefore we have two ways to solve this problem:
+ Add BGP to the ACL with the statement “permit tcp any any eq bgp”
+ Configure higher value for CIR in default class as 2Mbps is too low for web traffic (http & https)

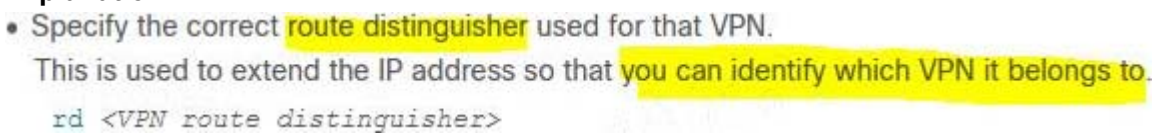
78.What is an advantage of using BFD?
A. It detects local link failure at layer 1 and updates routing table.
B. It detects local link failure at layer 2 and updates routing protocols.
C. It has sub-second failure detection for layer 1 and layer 3 problems.
D. It has sub-second failure detection for layer 1 and layer 2 problems.
Answer: D

79.Refer the exhibit.

```
R3#show policy-map control-plane

Service-policy output: R3_CoPP

  Class-map: mgmt (match-all)
    361 packets, 73858 bytes
    5 minute offered rate 0 bps, drop rate 0bps
    Match: access-group 20
    police:
        cir 8000 bps, bc 1500 bytes, be 1500 bytes
        conformed 8 packets, 1506 bytes; actions:
          transmit
        exceeded 353 packets, 72352 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps, violate 0 bps

  Class-map: class-default (match-any)
    124 packets, 10635 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
R3#show access-lists 120
Extended IP access list 120
    10 permit udp any any eq snmptrap (361 matches)
```

Which action resolves intermittent connectivity observed with the SNMP trap packets?
A. Decrease the committed burst Size of the mgmt class map
B. Increase the CIR of the mgmt class map
C. Add a new class map to match TCP traffic
D. Add one new entry in the ACL 120 to permit the UDP port 161
Answer: B

80.Which component of MPLS VPNs is used to extend the IP address so that an engineer is able to identify to which VPN it belongs?
A. VPNv4 address family
B. RD
C. RT
D. LDP
Answer: B
Explanation:



81.During the maintenance window an administrator accidentally deleted the Telnet-related configuration that permits a Telnet connection from the inside network (Eth0/0) to the outside of the networking between Friday – Sunday night hours only.
Which configuration resolves the issue?
A. interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
eq telnet time-range change window
!
time-range change window
periodic Friday Saturday Sunday 22:00 to 05:00
B. interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
eq telnet time-range change window
!
time-range change window
periodic 22:00 to 05:00
C. interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in

!
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
eq telnet time-range change window
!
time-range change window
periodic Friday Saturday Sunday 22:00 to 05:00
D. interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
eq telnet time-range change window
!
time-range change window
periodic Friday Saturday Sunday
Answer: C

82.An engineer configured a company's multiple area OSPF head office router and Site A cisco routers with VRF lite. Each site router is connected to a PE router of an MPLS backbone.

Head Office and Site A:
ip cef
ip vrf abc
rd 101:101
!
interface FastEthernet0/0
ip vrf forwarding abc
ip address 172.16.16.x 255.255.255.252
!
router ospf 1 vrf abc
log-adjacency-changes
network 172.16.16.0 0.0.0.255 area 1

After finishing both site router configurations, none of the LSA 3,4 5, and 7 are installed at Site A router. Which configuration resolves this issue?
A. configure capability vrf-lite on Site A and its connected PE router under router ospf 1 vrf abc
B. configure capability vrf-lite on Head Office and its connected PE router under router ospf 1 vrf abc
C. configure capability vrf-lite on both PE routers connected to Head Office and Site A routers under routtr ospf 1 vrf abc
D. configure capability vrf-lite on Head Office and Site A routers under router ospf 1 vrf abc
Answer: C

83.Refer to the exhibit.

```
ip access-list extended FILTER
deny tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 22
deny tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 23
deny tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 80
deny tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 443
permit tcp host 192.168.10.10 host 192.168.100.10 eq ssh
permit ip any any
!
interface GigabitEthernet0/1
ip address 192.168.10.1 255.255.255.0
ip access-group FILTER in
```

The ACL is placed on the inbound Gigabit 0/1 interface of the router. Host 192.168.10.10cannot SSH to host 192.168.100.10 even though the flow is permitted.
Which action resolves the issue without opening full access to this router?
A. Move the SSH entry to the beginning of the ACL
B. Temporarily move the permit ip any any line to the beginning of the ACL to see if the flow works
C. Temporarily remove the ACL from the interface to see if the flow works
D. Run the show access-list FILTER command to view if the SSH entry has any hit statistic associated with it
Answer: A

84.Which security feature can protect DMVPN tunnels?
A. IPsec
B. TACACS+
C. RTBH
D. RADIUS
Answer: A

85.Which two methods use IPsec to provide secure connectivity from the branch office to the headquarters office? (Choose two.)
A. DMVPN
B. MPLS VPN
C. Virtual Tunnel Interface (VTI)
D. SSL VPN
E. PPPoE
Answer: AC

86.Which protocol is used in a DMVPN network to map physical IP addresses to logical IP addresses?
A. BGP
B. LLDP
C. EIGRP
D. NHRP
Answer: D

87.Which Cisco VPN technology can use multipoint tunnel, resulting in a single GRE tunnel interface on the hub, to support multiple connections from multiple spoke devices?
A. DMVPN
B. GETVPN
C. Cisco Easy VPN
D. FlexVPN
Answer: A

88.Which option is the best for protecting CPU utilization on a device?
A. fragmentation
B. COPP
C. ICMP redirects
D. ICMP unreachable messages
Answer: B

89.What is the role of a route distinguisher via a VRF-Lite setup implementation?
A. It extends the IP address to identify which VFP instance it belongs to.
B. It manages the import and export of routes between two or more VRF instances
C. It enables multicast distribution for VRF-Lite setups to enhance EGP routing protocol capabilities
D. It enables multicast distribution for VRF-Lite setups to enhance IGP routing protocol capabilities
Answer: A

90.Refer to the following output:
Router#show ip nhrp detail
10.1.1.2/8 via 10.2.1.2, Tunnel1 created 00:00:12, expire 01:59:47
TypE. dynamic, Flags: authoritative unique nat registered used
NBMA address: 10.12.1.2
What does the authoritative flag mean in regards to the NHRP information?
A. It was obtained directly from the next-hop server.
B. Data packets are process switches for this mapping entry.
C. NHRP mapping is for networks that are local to this router.
D. The mapping entry was created in response to an NHRP registration request.
E. The NHRP mapping entry cannot be overwritten.
Answer: A

91.Which two protocols can cause TCP starvation? (Choose two)
A. TFTP
B. SNMP
C. SMTP
D. HTTPS
E. FTP
Answer: AB

92.Which two statements about VRF-Lite configurations are true? (Choose two.)
A. They support the exchange of MPLS labels
B. Different customers can have overlapping IP addresses on different VPNs
C. They support a maximum of 512.000 routes
D. Each customer has its own dedicated TCAM resources
E. Each customer has its own private routing table.
F. They support IS-IS
Answer: BE

93.A network engineer needs to verify IP SLA operations on an interface that shows on indication of excessive traffic.
Which command should the engineer use to complete this action?
A. show frequency
B. show track
C. show reachability
D. show threshold
Answer: B

94.Which protocol does VRF-Lite support?
A. IS-IS
B. ODR
C. EIGRP
D. IGRP
Answer: C

95.Refer to Exhibit.

```
router ospf 10
  router-id 192.168.1.1
  log-adjacency-changes
  redistribute bgp 1 subnets route-map BGP-TO-OSPF
!
route-map BGP-TO-OSPF deny 10
  match ip address 50
route-map BGP-TO-OSPF permit 20
!
access-list 50 permit 172.16.1.0 0.0.0.255
```

Which statement about redistribution from BGP into OSPF process 10 is true?
A. Network 172.16.1.0/24 is not redistributed into OSPF.
B. Network 10.10 10.0/24 is not redistributed into OSPF
C. Network 172.16.1.0/24 is redistributed with administrative distance of 1.
D. Network 10.10.10.0/24 is redistributed with administrative distance of 20.
Answer: A

96.Which two statements about redistributing EIGRP into OSPF are true? (Choose two)

A. The redistributed EIGRP routes appear as type 3 LSAs in the OSPF database
B. The redistributed EIGRP routes appear as type 5 LSAs in the OSPF database
C. The administrative distance of the redistributed routes is 170
D. The redistributed EIGRP routes appear as OSPF external type 1
E. The redistributed EIGRP routes as placed into an OSPF area whose area ID matches the EIGRP autonomous system number
F. The redistributed EIGRP routes appear as OSPF external type 2 routes in the routing table
Answer: BF

97.Refer to the exhibit.

```
router eigrp 1

redistribute ospf 5 match external route-map OSPF-TO-EIGRP
metric 10000 2000 255 1 1500
route-map OSPF-TO-EIGRP
match ip address TO-OSPF
```

Which routes from OSPF process 5 are redistributed into EIGRP?
A. E1 and E2 subnets matching access list TO-OSPF
B. E1 and E2 subnets matching prefix list TO-OSPF
C. only E2 subnets matching access list TO-OSPF
D. only E1 subnets matching prefix listTO-OS1
Answer: A

98.Users were moved from the local DHCP server to the remote corporate DHCP server. After the move, none of the users were able to use the network.
Which two issues will prevent this setup from working properly? (Choose two)
A. Auto-QoS is blocking DHCP traffic.
B. The DHCP server IP address configuration is missing locally
C. 802.1X is blocking DHCP traffic
D. The broadcast domain is too large for proper DHCP propagation
E. The route to the new DHCP server is missing
Answer: BE

99.Which command is used to check IP SLA when an interface is suspected to receive lots of traffic with options?
A. show track
B. show threshold
C. show timer
D. show delay
Answer: A

100.Which SNMP verification command shows the encryption and authentication protocols that are used in SNMPV3?

A. show snmp group
B. show snmp user
C. show snmp
D. show snmp view
Answer: B

101.Which is statement about IPv6 inspection is true?
A. It teams and secures bindings for stateless autoconfiguration addresses in Layer 3 neighbor tables
B. It learns and secures bindings for stateful autoconfiguration addresses in Layer 3 neighbor tables
C. It teams and secures bindings for stateful autoconfiguration addresses in Layer 2 neighbor tables
D. It team and secures binding for stateless autoconfiguration addresses in Layer 2 neighbor tables.
Answer: D

102.What is the output of the following command:
show ip vrf
A. Show's default RD values
B. Displays IP routing table information associated with a VRF
C. Show's routing protocol information associated with a VRF.
D. Displays the ARP table (static and dynamic entries) in the specified VRF
Answer: A

103.Refer to the exhibit.

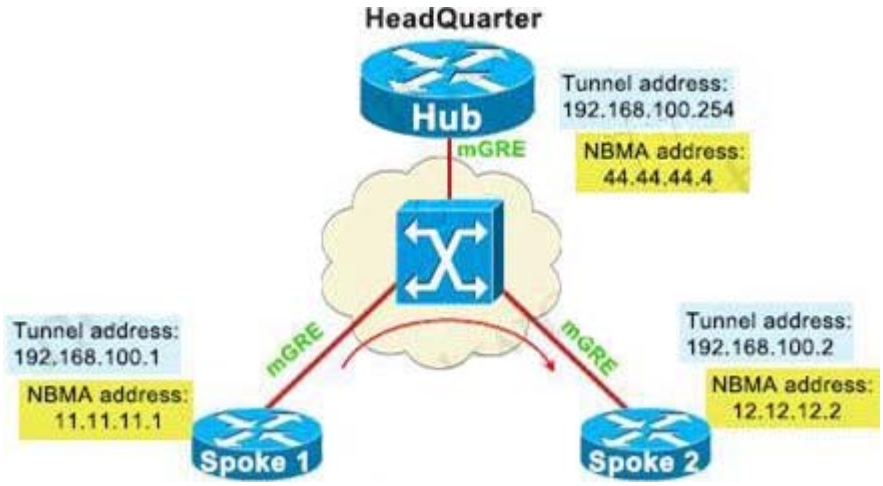
```
ip dhcp pool 1
 network 200.30.30.0/24
 default-router 200.30.30.100
 lease 40
!
ip dhcp pool 2
 network 200.30.40.0/24
 default-router 200.30.40.100
 lease 40
!
```

The server for the finance department is not reachable consistently on the 200.30.40.0/24 network and after every second month it gets a new IP address.
Which two actions must be taken to resolve this Issue? (Choose two.)
A. Configure the server to use DHCP on the network with default gateway 200 30.40.100.
B. Configure the server with a static IP address and default gateway.
C. Configure the router to exclude a server IP address.
D. Configure the server to use DHCP on the network with default gateway 200 30.30.100.
E. Configure the router to exclude a server IP address and default gateway.
Answer: B, C

104.Refer to the exhibit.

```
Device# show dmvpn
Tunnel0, Type:Spoke, NHRP Peers:2,
# Ent  Peer NBMA Addr  Peer Tunnel Add State  UpDn Tm  Attrb
-----  --------------  --------------- ------ --------  -----
    1  172.18.16.2     192.168.1.1     UP     01:33:23 S
    1  172.18.46.2     192.168.1.4     UP     00:23:03 D
```

An engineer has configured DMVPN on a spoke router.
What is the WAN IP address of another spoke router within the DMVPN network?
A. 172.18.46.2
B. 192.168.1.4
C. 172.18.16.2
D. 192.168.1.1
Answer: A
Explanation:
From the output we can see there are 2 NHRP Peers. The first one with the NBMA Address of 172.18.16.2 and the “Attribute” (Attrb) of Static (S) so we can deduce it is the Hub device.
Therefore the second one must be the remaining Spoke device with the attribute of Dynamic (D).



--> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========

Interface: Tunnel1, IPv4 NHRP Details
Type: Spoke, NHRP Peers:2,
Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 44.44.44.4 192.168.100.254 UP 00:03:40 S
1 12.12.12.2 192.168.100.2 UP 00:03:20 D

105.DRAG DROP
Drag and drop the MPLS VPN device types from me left onto the definitions on the right.

Customer (C) device	device in the enterprise network that connects to other customer devices
CE device	device in the core of the provider network that switches MPLS packets
PE device	device that attaches and detaches the VPN labels to the packets in the provider network
Provider (P) device	device at the edge of the enterprise network that connects to the SP network

Answer:

Customer (C) device	Provider (P) device
CE device	PE device
PE device	Customer (C) device
Provider (P) device	CE device

106.DRAG DROP

Drag and Drop the IPv6 First-Hop Security features from the left onto the definitions on the right.

IPv6 Binding Table	Block reply and advertisement messages from unauthorized DHCP servers and relay agents
IPv6 DHCPv6 Guard	Create a binding table that is based on NS and NA messages
IPv6 Source Guard	Filter inbound traffic on Layer 2 switch port that are not in the IPv6 binding table
IPv6 ND Inspection	Block a malicious host and permit the router from a legitimate route
IPv6 RA Guard	Create IPv6 neighbors connected to the device from information sources such as NDP snooping

Answer:

IPv6 Binding Table	IPv6 RA Guard
IPv6 DHCPv6 Guard	IPv6 DHCPv6 Guard
IPv6 Source Guard	IPv6 ND Inspection
IPv6 ND Inspection	IPv6 Source Guard
IPv6 RA Guard	IPv6 Binding Table

107.An engineer is configuring a network and needs packets to be forwarded to an interface for any destination address that is not in the routing table.
What should be configured to accomplish this task?
A. set ip next-hop
B. set ip default next-hop
C. set ip next-hop recursive
D. set ip next-hop verify-availability
Answer: B
Explanation:

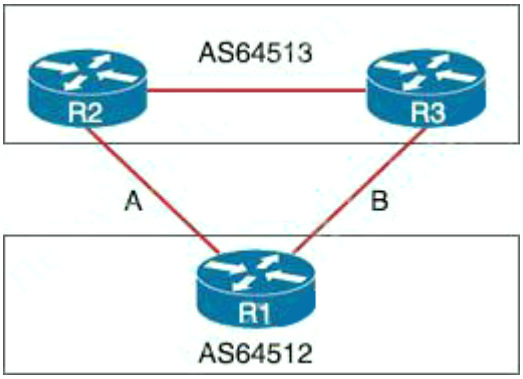
The **set ip default next-hop** command verifies the existence of the destination IP address in the routing table, and...

- if the destination IP address exists, the command does not policy route the packet, but forwards the packet based on the routing table.
- if the destination IP address does not exist, the command policy routes the packet by sending it to the specified next hop.

108.Which protocol does MPLS use to support traffic engineering?
A. Tag Distribution Protocol (TDP)
B. Resource Reservation Protocol (RSVP)
C. Border Gateway Protocol (BGP)
D. Label Distribution Protocol (LDP)
Answer: B
Explanation:

MPLS TE provides a way to integrate TE capabilities (such as those used on Layer 2 protocols like ATM) into Layer 3 protocols (IP). MPLS TE uses an extension to existing protocols (Intermediate System-to-Intermediate System (IS-IS), Resource Reservation Protocol (RSVP), OSPF) to calculate and establish unidirectional tunnels that are set according to the network constraint. Traffic flows are mapped on the different tunnels depending on their destination.

109.Refer to the exhibit.



A network engineer for AS64512 must remove the inbound and outbound traffic from link A during maintenance without closing the BGP session so that there ..... a backup link over link A toward the ASN.

Which BGP configuration on R1 accomplishes this goal?

A)

```
route-map link-a-in permit 10
 set weight 200
route-map link-a-out permit 10
 set as-path prepend 64512
route-map link-b-in permit 10
 set weight 100
route-map link-b-out permit 10
```

B)

```
route-map link-a-in permit 10
 set local-preference 200
route-map link-a-out permit 10
route-map link-b-in permit 10
route-map link-b-out permit 10
 set as-path prepend 64512
```

C)

```
route-map link-a-in permit 10
route-map link-a-out permit 10
 set as-path prepend 64512
route-map link-b-in permit 10
 set local-preference 200
route-map link-b-out permit 10
```

D)

```
route-map link-a-in permit 10
 set weight 200
route-map link-a-out permit 10
route-map link-b-in permit 10
 set weight 100
route-map link-b-out permit 10
 set as-path prepend 64512
```

A. Option A

B. Option B

C. Option C

D. Option D
Answer: C

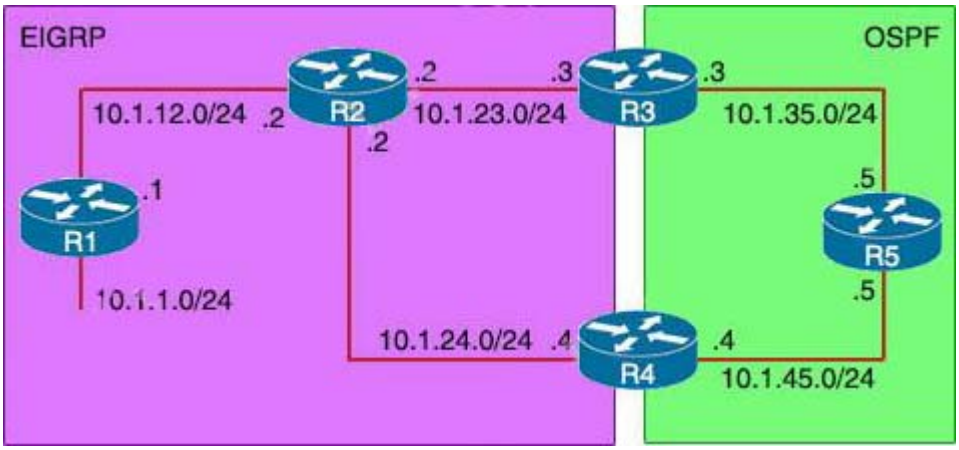
110. Topic 2, Exam Pool B

Refer to the exhibit.

```
R3#show policy-map control-plane
 Control Plane

  Service-policy output: R3_CoPP

   Class-map: SNMP-Out (match-all)
     124 packets, 3345 bytes
     5 minute offered rate 0 bps, drop rate 0bps
     Match: access-group name SNMP
     police:
         cir 8000 bps, bc 1500 bytes, be 1500 bytes
       conformed 0 packets, 0 bytes; actions:
         transmit
       exceeded 0 packets, 0 bytes; actions:
         drop
       conformed 0 bps, exceed 0 bps

   Class-map: class-default (match-any)
     10 packets, 1003 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: any
R1#show access-lists SNMP
Extended IP access list SNMP
    10 permit udp any eq snmp any
```

R1 is being monitored using SNMP and monitoring devices are getting only partial information.
What action should be taken to resolve this issue?
A. Modify the CoPP policy to increase the configured exceeded limit for SNMP.
B. Modify the access list to include snmptrap.
C. Modify the CoPP policy to increase the configured CIR limit for SNMP.
D. Modify the access list to add a second line to allow udp any any eq snmp
Answer: D

111.Refer to the exhibit.




```
R1
router eigrp 1
 redistribute connected
 network 10.1.12.1 0.0.0.0
 default-metric 1000000 10 255 1 1500

R3
router eigrp 1
 network 10.1.23.3 0.0.0.0
!
router ospf 1
 redistribute eigrp 1 subnets
 network 10.1.35.0 0.0.0.0 area 0
```

To provide reachability to network 10.1.1.0 /24 from R5, the network administrator redistributes EIGRP into OSPF on R3 but notices that R4 is now taking a ..... path through R5 to reach 10.1.1.0/24 network.

Which action fixes the issue while keeping the reachability from R5 to 10.1.1.0/24 network?

A. Change the administrative distance of the external EIGRP to 90.

B. Apply the outbound distribution list on R5 toward R4 in OSPF.

C. Change the administrative distance of OSPF to 200 on R5.

D. Redistribute OSPF into EIGRP on R4

Answer: A

112.Refer to the exhibit.

```
*Jul 23 09:33:34.530: IF-EvD(GigabitEthernet0/0): reports state transition from DOWN to
DOWN
*Jul 23 09:33:35.525: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to down
*Jul 23 09:33:35.528: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from
DOWN to DOWN
*Jul 23 09:33:36.215: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from
DOWN to DOWN
*Jul 23 09:33:37.996: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to
up
*Jul 23 09:33:38.006: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from
DOWN to UP
*Jul 23 09:33:38.998: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
```

R1 is connected with R2 via GigabitEthernet0/0, and R2 cannot ping R1.
What action will fix the issue?
A. Fix route dampening configured on the router.
B. Replace the SFP module because it is not supported.
C. Fix IP Event Dampening configured on the interface.
D. Correct the IP SLA probe that failed.
Answer: C
Explanation:

The IP Event Dampening feature introduces a configurable exponential decay mechanism to suppress the effects of excessive interface flapping events on routing protocols and routing tables in the network. This feature allows the network operator to configure a router to automatically identify and selectively dampen a local interface that is flapping.

113.Which IGPs are supported by the MPLS LDP autoconfiguration feature?
A. RIPv2 and OSPF
B. OSPF and EIGRP
C. OSPF and ISIS
D. ISIS and RIPv2
Answer: C
Explanation:

The MPLS LDP Autoconfiguration feature enables you to globally enable Label Distribution Protocol (LDP) on every interface associated with an Interior Gateway Protocol (IGP) instance. This feature is supported on Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) IGPs. It provides

114.An engineer needs dynamic routing between two routers and is unable to establish OSPF adjacency. The output of the show ip ospf neighbor command shows that the neighbor state is EXSTART/EXCHANGE.
Which action should be taken to resolve this issue?
A. match the passwords
B. match the hello timers
C. match the MTUs

D. match the network types

Answer: C

Explanation:

Neighbors Stuck in Exstart/Exchange State

The problem occurs most frequently when attempting to run OSPF between a Cisco router and another vendor's router. The problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces don't match. If the router with the higher MTU sends a packet larger that the MTU set on the neighboring router, the neighboring router ignores the packet.0 When

115.Refer to the exhibit.

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group 101 in
!
time-range Office-hour
 periodic weekdays 08:00 to 17:00
!
access-list 101 permit tcp 10.0.0.0 0.0.0.0 172.16.1.0 0.0.0.255 eq ssh
time-range Office-hour
```

An IT staff member comes into the office during normal office hours and cannot access devices through SSH.

Which action should be taken to resolve this issue?

A. Modify the access list to use the correct IP address.

B. Configure the correct time range.

C. Modify the access list to correct the subnet mask

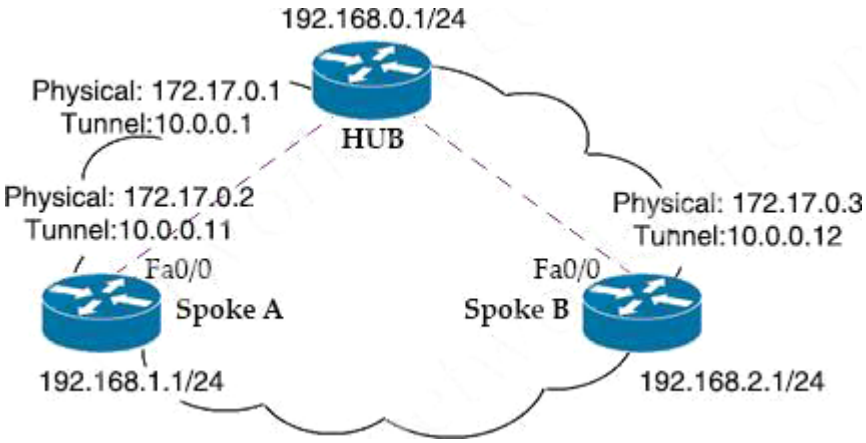
D. Configure the access list in the outbound direction.

Answer: A

Explanation:

To ACL should be permit tcp 101 10.1.1.1 0.0.0.0

116.Refer to the exhibit.



Which interface configuration must be configured on the HUB router to enable MVPN with mGRE mode?

Option A	Option B
interface Tunnel0 description mGRE – DMVPN Tunnel ip address 10.1.0.1 255.255.255.0 ip nhrp map multicast dynamic ip nhrp network-id 1 tunnel source 172.17.0.1 ip nhrp map 10.0.0.11 172.17.0.2 ip nhrp map 10.0.0.12 172.17.0.3 tunnel mode gre	interface Tunnel0 description mGRE – DMVPN Tunnel ip address 10.0.0.1 255.255.255.0 ip nhrp map multicast dynamic ip nhrp network-id 1 tunnel source 10.0.0.1 tunnel mode gre multipoint
Option C	**Option D**
interface Tunnel0 description mGRE – DMVPN Tunnel ip address 10.0.0.1 255.255.255.0 ip nhrp network-id 1 tunnel source 172.17.0.1 tunnel mode gre multipoint	interface Tunnel0 description mGRE – DMVPN Tunnel ip address 10.0.0.1 255.255.255.0 ip nhrp map multicast dynamic ip nhrp network-id 1 tunnel source 10.0.0.1 tunnel destination 172.17.0.2 tunnel mode gre multipoint

A. Option A
B. Option B
C. Option C
D. Option D
Answer: C
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-dmvpn.html

117.What does IPv6 Source Guard utilize to determine if IPv6 source addresses should be forwarded?
A. ACE
B. ACLS
C. DHCP
D. Binding Table
Answer: D
Explanation:

IPv6 source guard is an interface feature between the populated binding table and data traffic filtering. This feature enables the device to deny traffic when it is originated from an address that is not stored in the binding table. IPv6 source guard does not inspect ND or DHCP packets; rather, it works

118.Refer to the exhibit.

```
R1#show run | begin line
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
transport preferred telnet
transport output none
stopbits 0 4
!
line vty 0 4
login
transport preferred telnet
transport input none
transport output telnet
R1#
R1#ssh -l cisco 192.168.12.2
%ssh connections not permitted from this terminal
R1#
```

An engineer receives this error message when trying to access another router m-band from the serial interface connected to the console of R1.
Which configuration is needed on R1 to resolve this issue?

Option A

R1(config)#line console 0
R1(config-line)#transport preferred ssh

Option B

R1(config)#line vty 0
R1(config-line)#transport output ssh

Option C

R1(config)#line vty 0
R1(config-line)#transport output ssh
R1(config-line)#transport preferred ssh

Option D

R1(config)#line console 0
R1(config-line)#transport output ssh

A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

Explanation:

https://community.cisco.com/t5/other-network-architecture/out-of-band-router-access/td-p/333295

The “transport output none” command prevents any protocol connection made from R1.
Therefore our SSH connection to 192.168.12.2 was refused. In order to fix this problem we can configure “transport output ssh” under “line console 0” of R1.
Note: The parameter “-l” specifies the username to log in as on the remote machine.

119.Refer to the exhibit.

```
Router#show access-lists
Standard IP access list 1
    10 permit 192.168.2.2 (1 match)
Router#
Router#show route-map
route-map RM-OSPF-DL, deny, sequence 10
  Match clauses:
    ip address (access-lists): 1
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
Router#
Router#show running-config | section ospf
router ospf 1
  network 192.168.1.1 0.0.0.0 area 0
  network 192.168.12.0 0.0.0.255 area 0
  distribute-list route-map RM-OSPF-DL in
Router#
```

Which two actions should be taken to access the server? (Choose two.)
A. Modify the access list to add a second line of permit ip any
B. Modify the access list to deny the route to 192.168.2.2.
C. Modify distribute list seq 10 to permit the route to 192.168.2.2.
D. Add a sequence 20 in the route map to permit access list 1.
E. Add a floating static route to reach to 192.168.2.2 with administrative distance higher than OSPF
Answer: BE

120.Refer to the exhibit.

```
Router#show running-config
Building configuration…
!
<output omitted>
!
hostname R1
!
ip domain-name networktut.com
!
crypto key generate rsa modulus 2048
!
username admin privilege 15 secret cisco123
!
access-list 1 permit 10.1.1.0 0.0.0.255
access-list 1 deny any log
!
line vty 0 15
access-list 1 in
login local
!
<output omitted>
!
end
```

A user cannot SSH to the router.
What action must be taken to resolve this issue?
A. Configure transport input ssh
B. Configure transport output ssh
C. Configure ip ssh version 2
D. Configure ip ssh source-interface loopback0
Answer: A
Explanation:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/security/configuration_guide/b_sec_152ex_2960-x_cg/b_sec_152ex_2960-x_cg_chapter_01001.html

121.Refer to the exhibit.

```
MASS-RTR#show running-oonfig
!
hostname MASS-RTR
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization commands 15 default local
!
username admin privilege 15 password 7 02362448281l5F3348
username cisco privilege 15 password 7 0607072C394A5B
archive
 log oonfig
  logging enable
  logging size 1000
!
interface GigabitEthernet0/0
 ip address dhcp
 duplex auto
 speed auto
!
line vty 0 4
!

MASS-RTR#show archive log config all
idx   sess        user@line       Logged command
  1      1     console@console   |interface GigabitEthernet0/0
  2      1     console@console   | no shutdown
  3      1     console@console   | ip address dhcp
  4      2       admin@vty0      | username cisco privilege 15 password cisco
  5      2       admin@vty0      |!config: USER TABLE MODIFIED
```

A client is concerned that passwords are visible when running this show archive log config all.
Which router configuration is needed to resolve this issue?

A. MASS-RTR(config-archive-log-cfg)#password encryption aes

B. MASS-RTR(config)#aaa authentication arap

C. MASS-RTR(config)#service password-encryption

D. MASS-RTR(config-archive-log-cfg)#hidekeys

Answer: D

Explanation:

Step 7	**hidekeys** **Example:** `Device(config-archive-log-config)# hidekeys`	(Optional) Suppresses the display of password information in configuration log files. **Note** Enabling the **hidekeys** command increases security by preventing password information from being displayed in configuration log files.

122.Refer to the exhibit.

```
R1
ip prefix-list ccnp1 seq 5 permit 10.1.48.0/24 le 24
ip prefix-list ccnp2 seq 5 permit 10.1.80.0/24 le 32
ip prefix-list ccnp3 seq 5 permit 10.1.64.0/24 le 24

route-map ospf-to-eigrp permit 10
 match ip address prefix-list ccnp1
 set tag 30
route-map ospf-to-eigrp permit 20
 match ip address prefix-list ccnp2
 set tag 20
route-map ospf-to-eigrp permit 30
 match ip address prefix-list ccnp3
 set tag 10
```

An engineer wanted to set a tag of 30 to route 10 1.80.65/32 but it failed How is the issue fixed?

A. Modify route-map ospf-to-eigrp permit 30 and match prefix-list ccnp2.

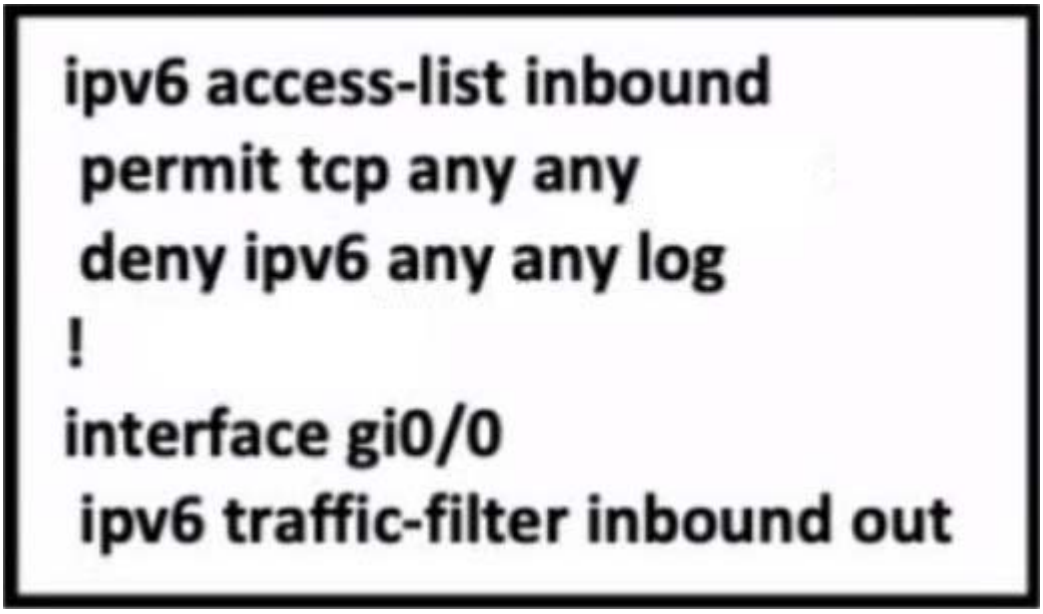
B. Modify route-map ospf-to-eigrp permit 10 and match prefix-list ccnp2.

C. Modify prefix-list ccnp3 to add 10.1.64.0/20 le 24

D. Modify prefix-list ccnp3 to add 10.1.64.0/20 ge 32

Answer: B

123.Refer to the exhibit.



A network administrator configured an IPv6 access list to allow TCP return frame only, but it is not working as expected.

Which changes resolve this issue?

A)

```
ipv6 access-list inbound
 permit tcp any any established
 deny ipv6 any any log
!
interface gi0/0
 ipv6 traffic-filter inbound out
```

B)

```
ipv6 access-list inbound
 permit tcp any any syn
 deny ipv6 any any log
!
interface gi0/0
 ipv6 traffic-filter inbound out
```

C)

```
ipv6 access-list inbound
 permit tcp any any established
 deny ipv6 any any log
!
interface gi0/0
 ipv6 traffic-filter inbound in
```

D)

```
ipv6 access-list inbound
 permit tcp any any syn
 deny ipv6 any any log
!
interface gi0/0
 ipv6 traffic-filter inbound in
```

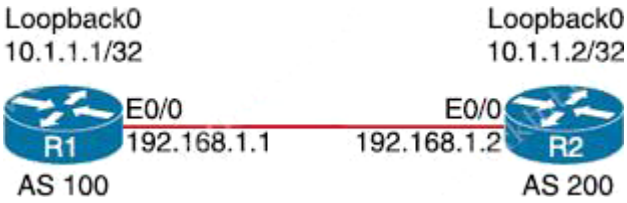
A. Option A
B. Option B
C. Option C
D. Option D
Answer: C
Explanation:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/122_55_se/configuration/guide/scg3750/swv6acl.html

124.What does the PE router convert the Ipv4 prefix to within an MPLS VPN?
A. VPN-IPv4 prefix combined with the 64-bit route distinguisher
B. 48-bit route combining the IP and PE router-id
C. prefix that combines the ASN, PE router-id, and IP prefix
D. eBGP path association between the PE and CE sessions
Answer: A
Explanation:

The IP prefix is a member of the IPv4 address family. After the PE device learns the IP prefix, the PE converts it into a VPN-IPv4 prefix by combining it with an 8-byte route distinguisher (RD). The generated prefix is a member of the VPN-IPv4 address family. It uniquely identifies the customer address, even if the customer site is using globally nonunique (unregistered private) IP addresses. The route distinguisher used to generate the VPN-IPv4 prefix is specified by a configuration command associated with the virtual routing and forwarding (VRF) instance on the PE device.

125.How are MPLS Layer 3 VPN services deployed?
A. The RD and RT values must match under the VRR
B. The RD and RT values under a VRF must match on the remote PE router
C. The import and export RT values under a VRF must always be the same.
D. The label switch path must be available between the local and remote PE routers.
Answer: D
Explanation:
https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/vpn/65x/b-l3vpn-cg-ncs5500-65x/b-l3vpn-cg-ncs5500-65x_chapter_010.html
The ingress PE router must be able to reach the egress PE router for a packet to be relayed to its destination.

126.Refer to the exhibit.



The R1 and R2 configurations are:

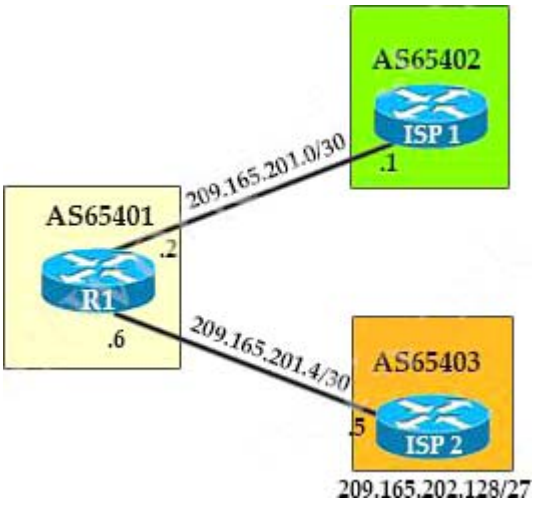
R1	R2
router bgp 100 neighbor 10.1.1.2 remote-as 200	router bgp 200 neighbor 10.1.1.1 remote-as 100

The neighbor is not coming up.
Which two sets of configurations bring the neighbors up? (Choose two.)
A. R2
ip route 10.1.1.1 255.255.255.255 192.168.1.1
!
router bgp 200
neighbor 10.1.1.1 tti-security hops 1
neighbor 10.1.1.1 update-source loopback 0
B. R2
ip route 10.1.1.1 255.255.255.255 192.168.1.1
!
router bgp 200
neighbor 10.1.1.1 disable-connected-check
neighbor 10.1.1.1 update-source loopback 0
C. R2
ip route 10.1.1.2 255.255.255.255 192.168.1.2
!

router bgp 100
neighbor 10.1.1.2 ttl-security hops 1
neighbor 10.1.1.2 update-source loopback 0
D. R1
ip route 10.1.1.2 255.255.255.255 192.168.1.2
!
router bgp 100
neighbor 10.1.1.1 ttl-security hops 1
neighbor 10.1.1.2 update-source loopback 0
E. R1
ip route 10.1.1.2 255.255.255.255 192.168.1.2
!
router bgp 100
neighbor 10.1.1.2 disable-connected-check
neighbor 10.1.1.2 update-source Loopback0
Answer: BE
Explanation:

The **neighbor disable-connected-check** command is used to disable the connection verification process for eBGP peering sessions that are reachable by a single hop but are configured on a loopback interface or otherwise configured with a non-directly connected IP address.

127.Refer to the exhibit.



```
R1
int G0/0
 ip address 209.165.201.2 255.255.255.252
int G0/1
 ip address 209.165.201.6 255.255.255.252
router bgp 65401
 bgp log-neighbor-changes
 redistribute static
 neighbor 209.165.201.1 remote-as 65402
 neighbor 209.165.201.5 remote-as 65403
ip route 209.165.200.224 255.255.255.224 Null0
ip route 209.165.202.128 255.255.255.224 Null0
```

A company with autonomous system number AS65401 has obtained IP address block 209.165.200.224/27 fro, ARIN. The company needed more IP addresses and was assigned block 209.165.202.128/27 from ISP2. An engineer is ISP1 reports they are receiving ISP2 routes from AS65401.

Which configuration onR1 resolves the issue?

A. access-list 10 deny 209.165.202.128 0.0.0.31
access-list 10 permit any
!
router bgp 65401
neighbor 209.165.201.1 distribute-list 10 out

B. access-list 10 deny 209.165.202.128 0.0.0.31
access-list 10 permit any
!
router bgp 65401
neighbor 209.165.201.1 distribute-list 10 in

C. ip route 209.165.200.224 255.255.255.224 209.165.201.1
ip route 209.165.202.128 255.255.255.224 209.165.201.5

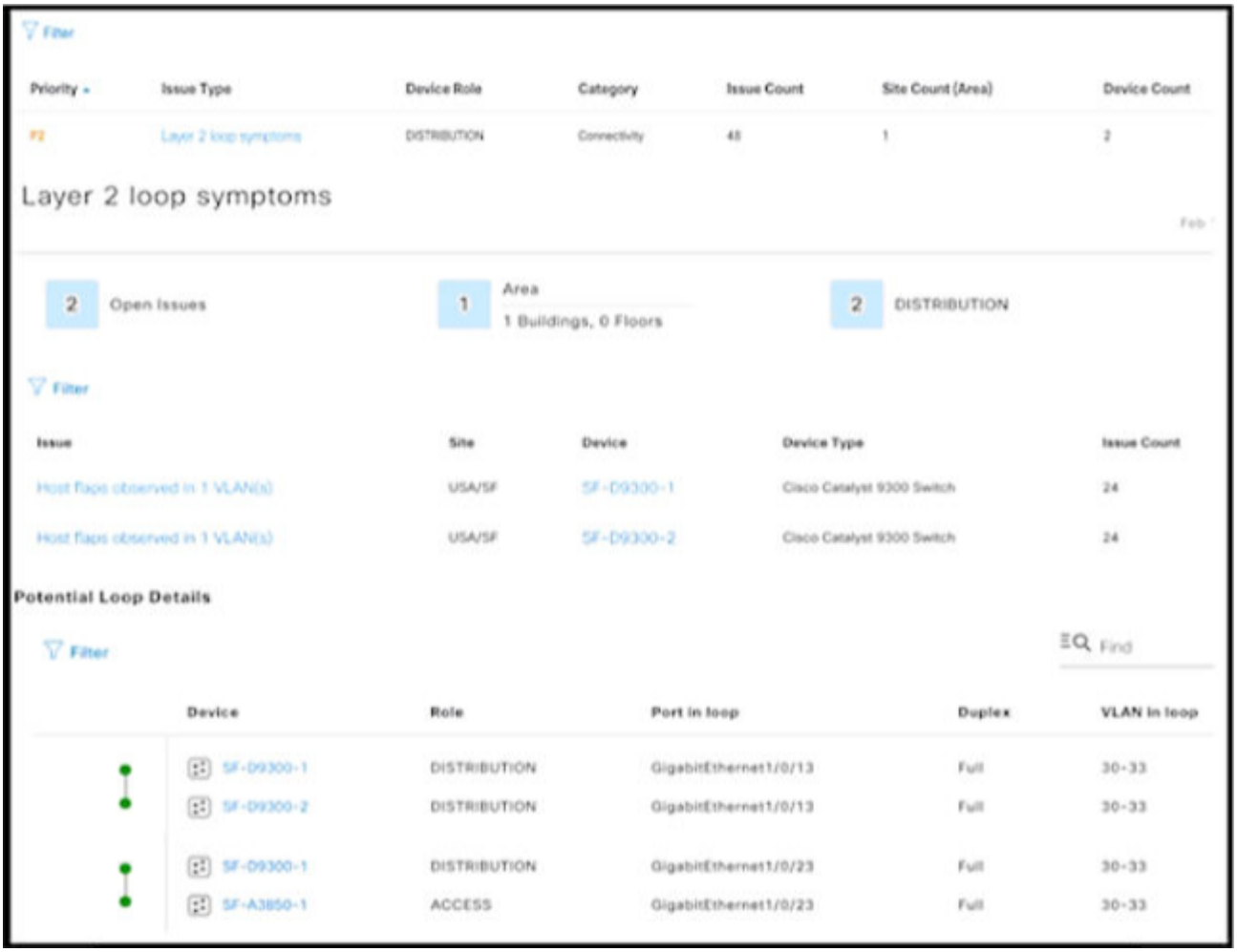
D. ip route 0.0.0.0 0.0.0.0 209.165.201.1
ip route 0.0.0.0 0.0.0.0 209.165.201.5

Answer: A

Explanation:

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/23675-27.html

128.Refer to the exhibit.



There is a picture of “Layer 2 loop symptoms” in DNAC and the config below:

```
interface GigabitEthernet1/0/13
 switchport trunk allowed vlan 30-33
 switchport mode trunk

int GigabitEthernet1/0/23
 switchport trunk allowed vlan 30-33
 switchport mode trunk
```

An engineer identifier a Layer 2 loop using DNAC.

Which command fixes the problem in the SF-D9300-1 switch?

A. no spanning-tree uplinkfast

B. spanning-tree loopguard default

C. spanning-tree backbonesfast

D. spanning-tree portfast bpduguard

Answer: D

Explanation:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dnacenter/tech_notes/b_dnac_sda_lan_automation_deployment.html

129.DRAG DROP
Drag and drop the actions from the left into the correct order on the right to configure a policy to avoid following packet forwarding based on the normal routing path.

configure set commands	Step 1
configure match commands	Step 2
configure fast switching for PBR	Step 3
configure route map instances	Step 4
configure PBR on the interface	Step 5
configure ACLs	Step 6

Answer:

configure set commands	configure ACLs
configure match commands	configure route map instances
configure fast switching for PBR	configure match commands
configure route map instances	configure set commands
configure PBR on the interface	configure PBR on the interface
configure ACLs	configure fast switching for PBR

Explanation:
https://community.cisco.com/t5/networking-documents/how-to-configure-pbr/ta-p/3122774

130.What are two functions of LDP? (Choose two.)
A. It is defined in RFC 3038 and 3039.
B. It requires MPLS Traffic Engineering.
C. It advertises labels per Forwarding Equivalence Class.
D. It must use Resource Reservation Protocol.
E. It uses Forwarding Equivalence Class
Answer: C E
Explanation:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/mpls/configuration/guide/mpls_cg/mp_mpls_overview.pdf

131.Refer to the exhibit.

A network administrator is using the DNA Assurance Dashboard panel to troubleshoot an OSPF adjacency that failed between Edge_NYC interface GigabitEthernet1/3 with Neighbor Edge_SNJ. The administrator observes that the neighborship is stuck in exstart state.

How does the administrator fix this issue?

A. Configure to match the OSPF interface speed and duplex settings on both routers.

B. Configure to match the OSPF interface MTU settings on both routers.

C. Configure to match the OSPF interface unique IP address and subnet mask on both routers.

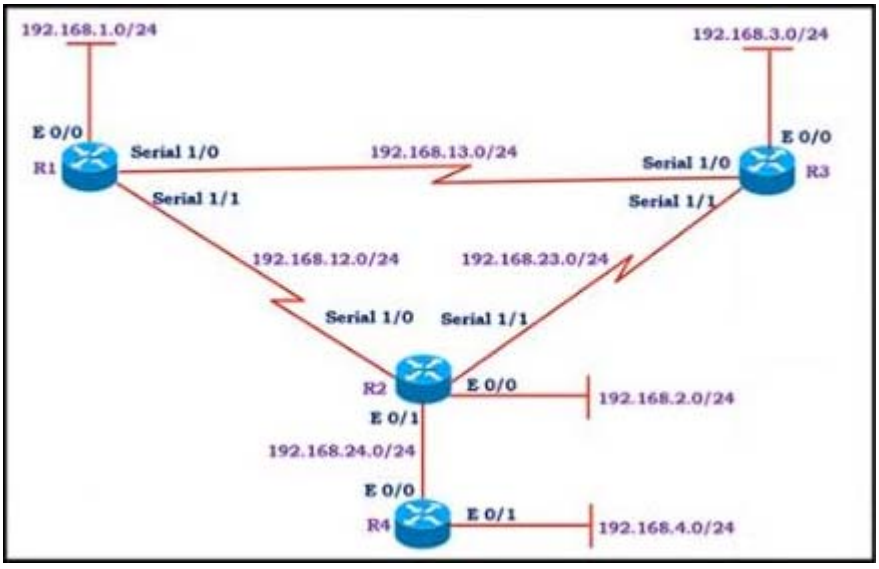
D. Configure to match the OSPF interface network types on both routers.

Answer: B

Explanation:

https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13684-12.html

132.Refer to the exhibit.



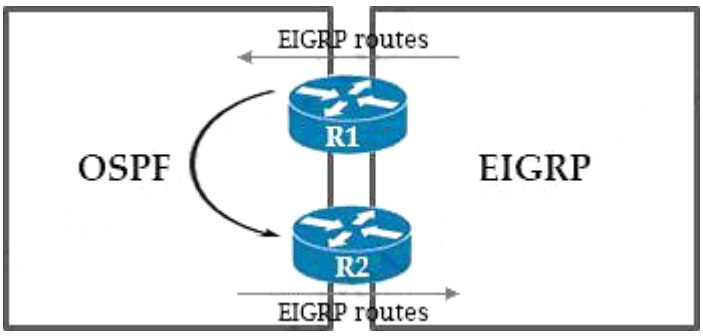
Show IP route on R1

```
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.1.0/24 is directly connected, Ethernet0/0
L   192.168.1.1/32 is directly connected, Ethernet0/0
D   192.168.2.0/24 [90/2297856] via 192.166.12.2.00:02:14, Serial1/1
S   192.168.3.0/24 [1/0] via 192.168.12.2
  192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.12.0/24 is directly connected, Serial1/1
L   192.168.12.1/32 is directly connected, Serial1/1
  192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.13.0/24 is directly connected, Serial1/0
L   192.168.13.1/32 is directly connected, Serial1/0
D   192.168.23.0/24 [90/2681856] via 192.168.13.3,00:06:38, Serial1/0
      [90/2681856] via 192.168.12.2, 00:06:38, Serial1/1
D   192.168.24.0/24 [90/2195456] via 192.168.12.2, 00:06:38, Serial1/1
```

All the serial between R1, R2, and R3 have the Same bandwidth. User on the 192.168.1.0/24 network report slow response times while they access resource on network 192.168.3.0/24. When a traceroute is run on the path. It shows that the packet is getting forwarded via R2 to R3 although the link between R1 and R3 is still up.
What must the network administrator to fix the slowness?
A. Change the Administrative Distance of EIGRP to 5.
B. Add a static route on R1 using the next hop of R3.
C. Remove the static route on R1.
D. Redistribute theR1 route to EIGRP
Answer: C

133.An engineer configured a Cisco router to send reliable and encrypted notifications for any events to the management server. It was noticed that the notification messages are reliable but not encrypted. Which action resolves the issue?
A. Configure all devices for SNMPv3 informs with priv.
B. Configure all devices for SNMPv3 informs with auth.
C. Configure all devices for SNMPv3 traps with auth.
D. Configure all devices for SNMPv3 traps with priv.
Answer: A
Explanation:
SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when this device receives traps.”Send reliable and encrypted notifications for any events” so it is SNMP notifications. For encryption we need to configure “priv”.

134.Refer to the exhibit.



A network administrator configured mutual redistribution on R1 and R2 routers, which caused instability in the network.

Which action resolves the issue?

A. Set a tag in the route map when redistributing EIGRP into OSPF on R1. and match the same tag on R2 to allow when redistributing OSPF into EIGRP.

B. Apply a prefix list of EIGRP network routes in OSPF domain on R1 to propagate back into the EIGRP routing domain.

C. Set a tag in the route map when redistributing EIGRP into OSPF on R1, and match the same tag on R2 to deny when redistributing OSPF into EIGRP.

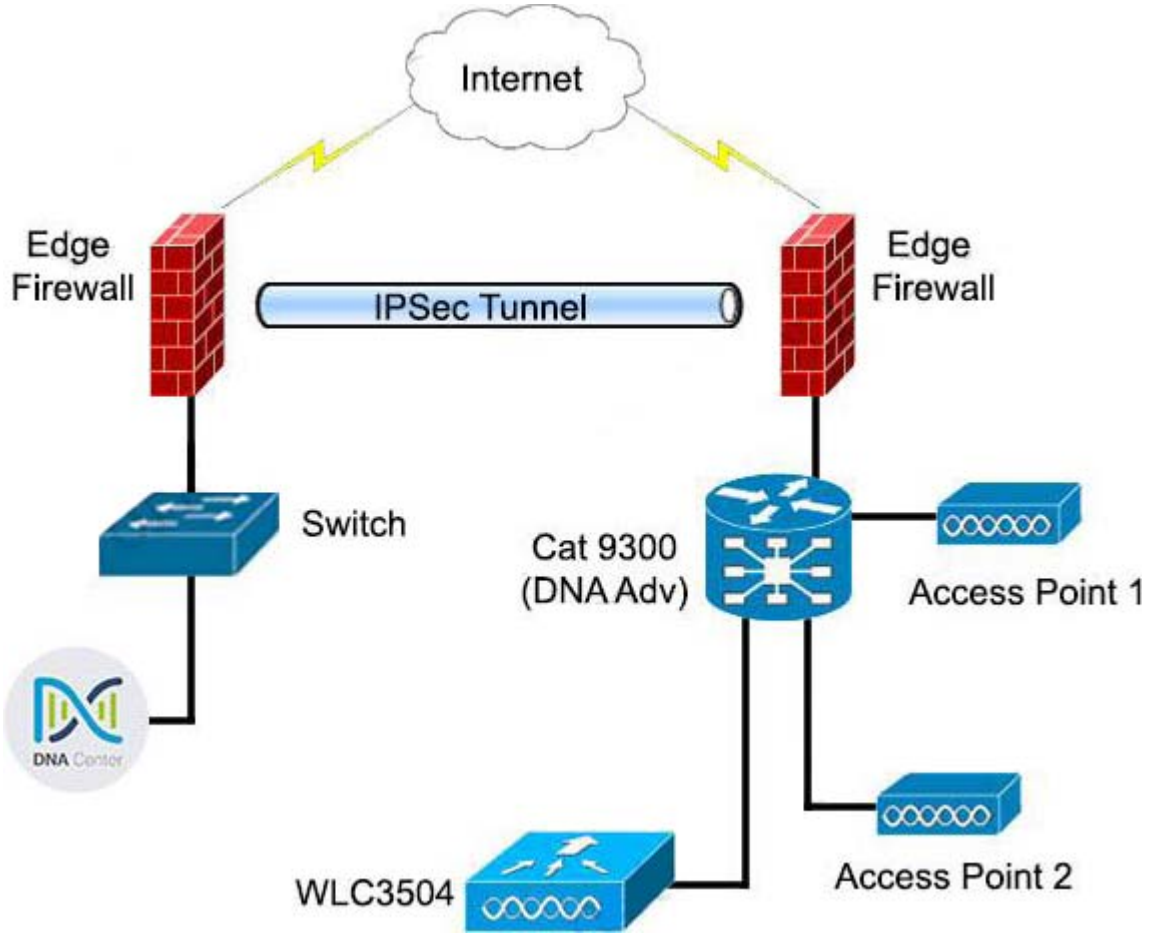
D. Advertise summary routes of EIGRP to OSPF and deny specific EIGRP routes when redistributing into OSPF.

Answer: C

Explanation:

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.html

135.Refer to the exhibit.

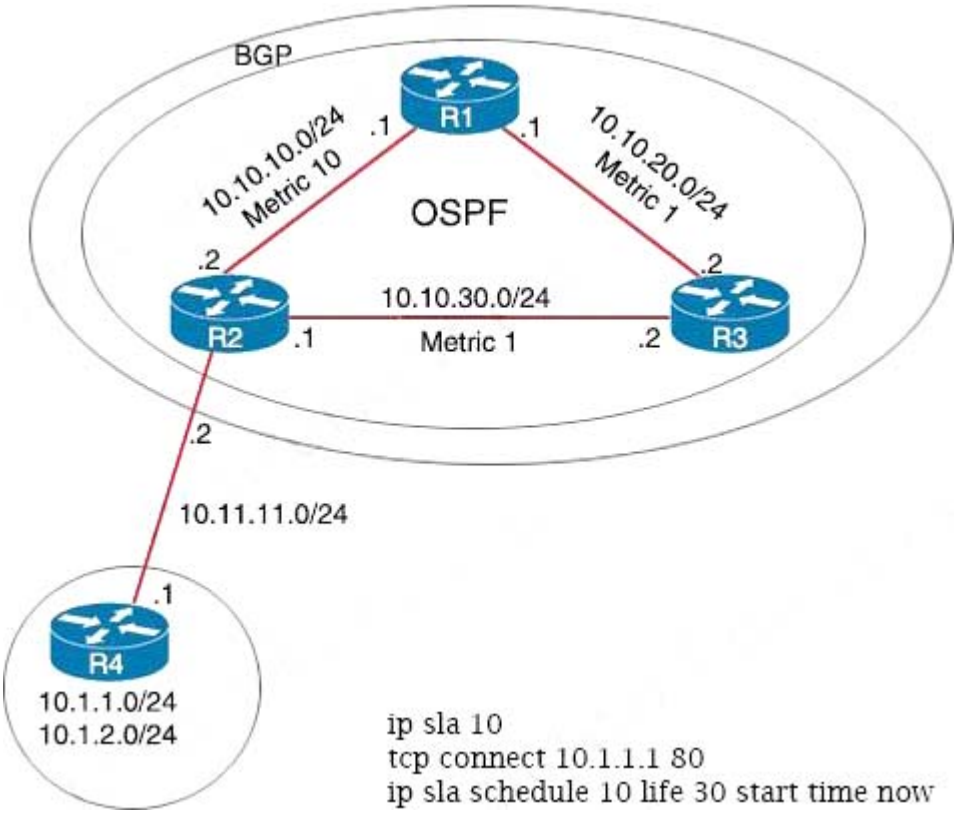


A network administrator is discovering a Cisco Catalyst 9300 and a Cisco WLC 3504 in Cisco DNA Center. The Catalyst 9300 is added successfully However the WLC is showing [error "uncontactable" when the administrator tries to add it in Cisco DNA Center.
Which action discovers WLC in Cisco DNA Center successfully?
A. Copy the .cert file from the Cisco DNA Center on the USB and upload it to the WLC 3504.
B. Delete the WLC 3504 from Cisco DNA Center and add it to Cisco DNA Center again.
C. Add the WLC 3504 under the hierarchy of the Catalyst 9300 connected devices.
D. Copy the .pern file from the Cisco DNA Center on the USB and upload it to the WLC 3504.
Answer: D
Explanation:
https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html#anc12

136.Which feature drops packets if the source address is not found in the snooping table?
A. IPv6 Source Guard
B. IPv6 Destination Guard
C. IPv6 Prefix Guard
D. Binding Table Recovery
Answer: A
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-3s/ip6f-xe-3s-book/ip6-

snooping.pdf

137.Refer to the exhibit.



A user has set up an IP SLA probe to test if a non-SLA host web server on IP address 10.1.1.1 accepts HTTP sessions prior to deployment. The probe is failing.
Which action should the network administrator recommend for the probe to succeed?
A. Re-issue the ip sla schedule command.
B. Add icmp-echo command for the host.
C. Add the control disable option to the tcp connect.
D. Modify the ip sla schedule frequency to forever.
Answer: C

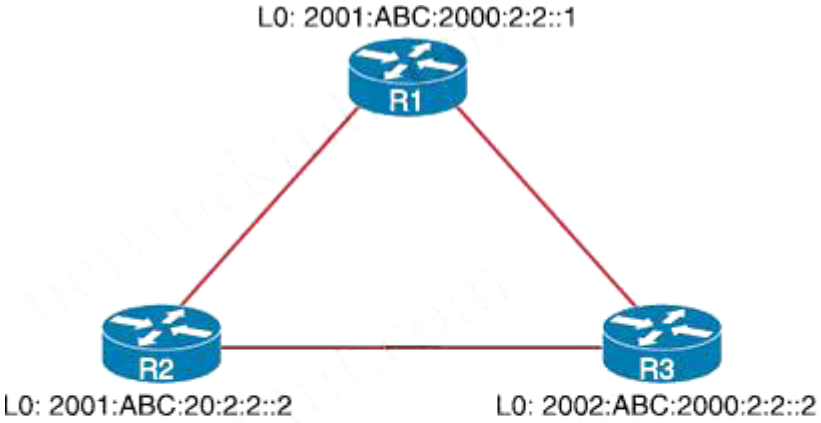
138.Refer to the exhibit.

The network administrator must mutually redistribute routes at the Chicago router to the LA and NewYork routers.
The configuration of the Chicago router is this:

```
router ospf 1
 redistribute eigrp 100
router eigrp 100
 redistribute ospf 1
```

After the configuration, the LA router receives all the NewYork routes, but NewYork router does not receive any LA routes.
Which set of configurations fixes the problem on the Chicago router?
A. router ospf 1
redistribute eigrp 100 metric 20
B. router eigrp 100
redistribute ospf 1 metric 10 10 10 10 10
C. router eigrp 100
redistribute ospf 1 subnets
D. router ospf 1
redistribute eigrp 100 subnets
Answer: B

139.Refer to the exhibit.




```
IPv6 access list PERMIT_SSH
 10 deny tcp 2001:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 23
 20 permit tcp 2001:ABC:2000:2:2::/64 host 2000:ABC:20:2:2::2 eq 22
 30 deny tcp 2002:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 22
 40 permit tcp 2000:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 22
 50 permit tcp 2000:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 23
 60 permit tcp host 2002:ABC:2000:2:2::2 host 2000:ABC:20:2:2::2 eq 22
 70 deny ipv6 any any
```

An IPv6 network was newly deployed in the environment and the help desk reports that R3 cannot SSH to the R2s Loopback interface.
Which action resolves the issue?
A. Modify line 10 of the access list to permit instead of deny.
B. Remove line 60 from the access list.
C. Modify line 30 of the access list to permit instead of deny.
D. Remove line 70 from the access list.
Answer: C

140.An engineer configured SNMP notifications sent to the management server using authentication and encrypting data with DES. An error in the response PDU is received as "UNKNOWNUSERNAME. WRONGDIGEST".

Which action resolves the issue?

A. Configure the correct authentication password using SNMPv3 authPriv .

B. Configure the correct authentication password using SNMPv3 authNoPriv.

C. Configure correct authentication and privacy passwords using SNMPv3 authNoPriv.

D. Configure correct authentication and privacy passwords using SNMPv3 authPriv.

Answer: D

Explanation:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-snmpv3.html

141.Refer to the exhibits.


```
Chicago Router
ip route 192.168.1.0 255.255.255.0 10.1.1.2
ip route 192.168.2.0 255.255.255.0 10.1.1.2
!
router eigrp 100
 redistribute static

LA router
 ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

A user on the 192.168.1.0/24 network can successfully ping 192.168.3.1, but the administrator cannot ping 192.168.3.1 from the LA router.

Which set of configurations fixes the issue?

A)

```
Chicago Router

router eigrp 100
 redistribute static metric 10 10 10 10 10
```

B)

```
Chicago Router

router eigrp 100
   redistribute connected
```

C)

```
Chicago Router

ip route 192.168.3.0 255.255.255.0 10.1.2.2
ip route 192.168.4.0 255.255.255.0 10.1.2.2
```

D)

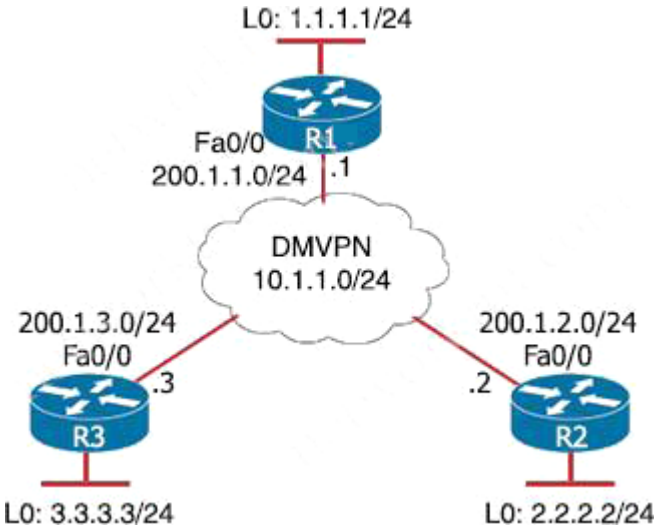
LA Router

ip route 192.168.3.0 255.255.255.0 10.1.1.1
ip route 192.168.4.0 255.255.255.0 10.1.1.1

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

142.Refer to the exhibits.



R2:

```
R2(config)# crypto isakmp policy 10
R2(config-isakmp)# hash md5
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)# encryption 3des
R2(config)# crypto ipsec transform-set TSET esp-des esp-md5-hmac
R2(cfg-crypto-trans)# mode transport
R2(config)# crypto ipsec profile TST
R2(ipsec-profile)# set transform-set TSET
R2(config)# interface tunnel 123
R2(config-if)# tunnel protection ipsec profile TST
```

When DMVPN is configured, which configuration allows spoke-to-spoke communication using loopback as a tunnel source?

A. Configure crypto isakmp key cisco address 0.0.0.0 on the hub.
B. Configure crypto isakmp key Cisco address 200.1.0.0 255.255.0.0 on the hub.
C. Configure crypto isakmp key cisco address 200.1.0.0 255.255.0.0 on the spokes.
D. Configure crypto isakmp key cisco address 0.0.0.0 on the spokes.

Answer: D

Explanation:

https://www.cisco.com/en/US/technologies/tk583/tk372/technologies_white_paper0900aecd802b8f3c.html

143.What are two functions of IPv6 Source Guard? (Choose two.)
A. It uses the populated binding table for allowing legitimate traffic.
B. It works independent from IPv6 neighbor discovery.
C. It denies traffic from unknown sources or unallocated addresses.
D. It denies traffic by inspecting neighbor discovery packets for specific pattern.
E. It blocks certain traffic by inspecting DHCP packets for specific sources.
Answer: A C
Explanation:

IPv6 source guard is an interface feature between the populated binding table and data traffic filtering.

IPv6 source guard can deny traffic from unknown sources or unallocated addresses,

144.An engineer configured access list NON-CISCO in a policy to influence routes

```
route-map PBR, deny, sequence 5
  Match clauses:
    ip address (access-list): NON-CISCO
  Set clauses:
Policy routing matches: 0 packets, 0 bytes
route-map PBR, permit, sequence 10
  Match clauses:
  Set clauses:
    ip next-hop 192.168.1.5
  Policy routing matches: 389202995 packets, 222006352077 bytes
```

What are the two effects of this route map configuration? (Choose two.)
A. Packets are not evaluated by sequence 10.
B. Packets are evaluated by sequence 10.
C. Packets are forwarded to the default gateway.
D. Packets are forwarded using normal route lookup.
E. Packets are dropped by the access list.
Answer: BC
Explanation:
https://www.cisco.com/c/en/us/support/docs/ip/ip-routed-protocols/47121-pbr-cmds-ce.html

145.DRAG DROP
Drag and drop the MPLS VPN device types from the left onto the definitions on the right.

Customer (C) device	device in the enterprise network that connects to other customer devices
CE device	device in the core of the provider network that switches MPLS packets
PE device	device that attaches and detaches the VPN labels to the packets in the provider network
Provider (P) device	device at the edge of the enterprise network that connects to the SP network

Answer:

Customer (C) device	Customer (C) device
CE device	Provider (P) device
PE device	PE device
Provider (P) device	CE device

146.Refer to the exhibit.

```
R1# show policy-map control-plane
Control plane
 service-plane input: CoPP
 class-map: PERMIT (match-all)
  50 packets, 3811 bytes
  5 minute offered rate 0000 bps
  Match: access-group 100
 class-map: ANY (match-all)
  210 packets, 19104 bytes
  5 minute offered rate 0000 bps, drop rate 0000bps
  Match: access-group 199
   drop
 class-map: class-default (match-any)
  348 packets, 48203 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: any

R1#show access-list 100
Extended IP access list 100
 10 permit udp any any eq 23 (100 matches)
 20 permit tcp any any eq telnet (5 matches)
 30 permit tcp any eq telnet any (10 matches)

R1#show access-list 199
Extended IP access 199
 10 deny tcp any eq telnet any (50 matches)
 50 permit ip any any (1 match)

R1# show run | section line vty
line vty 0 4
 login
 transport input telnet ssh
 transport output telnet ssh
```

Which two actions restrict access to router R1 by SSH? (Choose two.)

A. Configure transport input ssh on line vty and remove sequence 30 from access list 100.

B. Configure transport output ssh on line vty and remove sequence 20 from access list 100.

C. Remove class-map ANY from service-policy CoPP

D. Configure transport output ssh on line vty and remove sequence 10 from access list 199.

E. Remove sequence 10 from access list 100 and add sequence 20 deny tcp any any eq telnet to access list 199

Answer: AB

147.What is the minimum time gap required by the local system before putting a BFD control packet on the wire?
A. Detect Mult
B. Required Min Echo RX Interval
C. Desired Min TX Interval
D. Required Min RX Interval
Answer: C
Explanation:
Desired Min TX Interval: This is the minimum interval, in microseconds, that the local system would like to use when transmitting BFD Control packets, less any jitterapplied. The value zero is reserved.
Required Min Echo RX Interval: This is the minimum interval, in microseconds, between received BFD Echo packets that this system is capable of supporting, less anyjitter applied by the sender. If this value is zero, the transmitting system does not support the receipt of BFD Echo packets.
Reference: https://tools.ietf.org/html/rfc5880

148.Refer to the exhibit.

```
login block-for 15 attempts 10 within 120
login on-failure log
login on-success log
archive
log config
logging enable
logging size 300
notify syslog
snmp-server enable traps syslog
snmp-server host 172.16.17.1 public syslog
```

The administrator can see the traps for the failed login attempts, but cannot see the traps of successful login attempts.
What command is needed to resolve the issue?
A. Configure logging history 2
B. Configure logging history 3
C. Configure logging history 4
D. Configure logging history 5
Answer: D
Explanation:
By default, the maximum severity sent as a syslog trap is warning. That is why you see syslog traps for login failures. Since a login success is severity 5 (notifications), those syslog messages will not be converted to traps.
To fix this, configure:

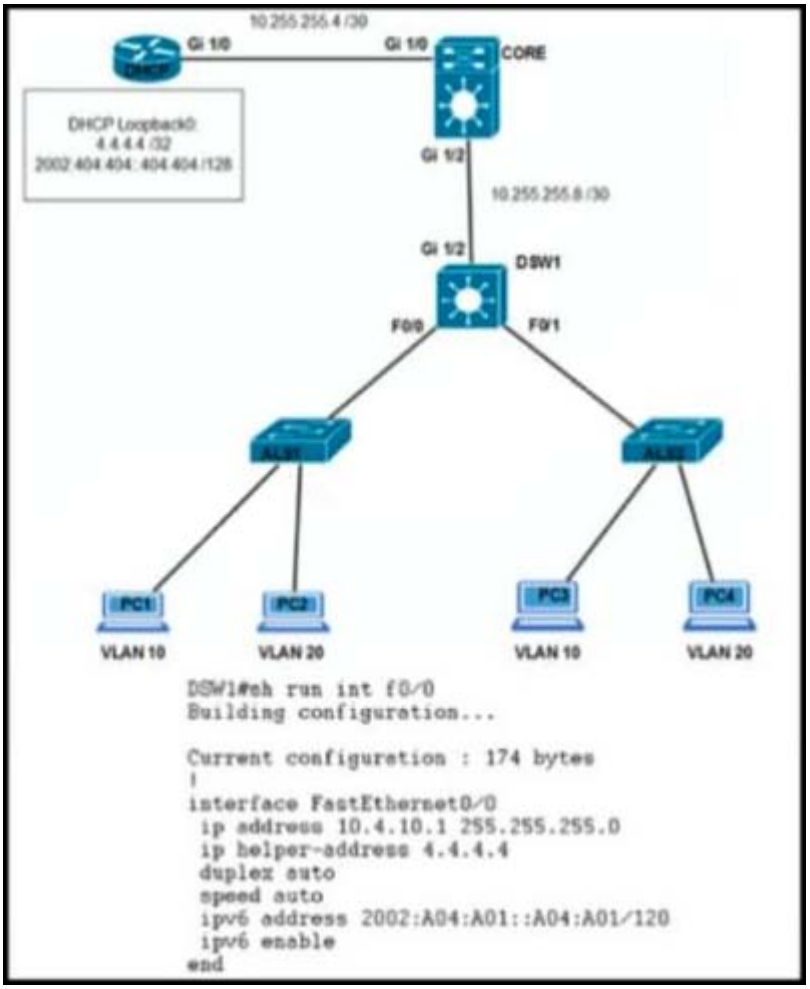
logging history 5

Syslog levels are listed below

Level	Keyword	Description
0	emergencies	System is unusable
1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist
6	informational	Informational messages
7	debugging	Debugging messages

Note:
The syntax of login block is:
login block-for seconds attempts tries within seconds

149.Clients on ALS2 receive IPv4 and IPv6 addresses but clients on ALS1 receive only IPv4 addresses and not IPv6 addresses.
Which action on DSW1 allows clients on ALS1 to receive IPv6 addresses?



Configure DSW1(dhcp-config)#**default-router 2002:A04:A01::A04:A01**

Configure DSW1(config-if)#**ipv6 dhcp relay destination 2002:404:404::404:404 GigabitEthernet1/2**

Configure DSW1(config)#**ipv6 route 2002:404:404::404:404/128 FastEthernet1/0**

Configure DSW1(config-if)#**ipv6 helper address 2002:404:404::404:404**

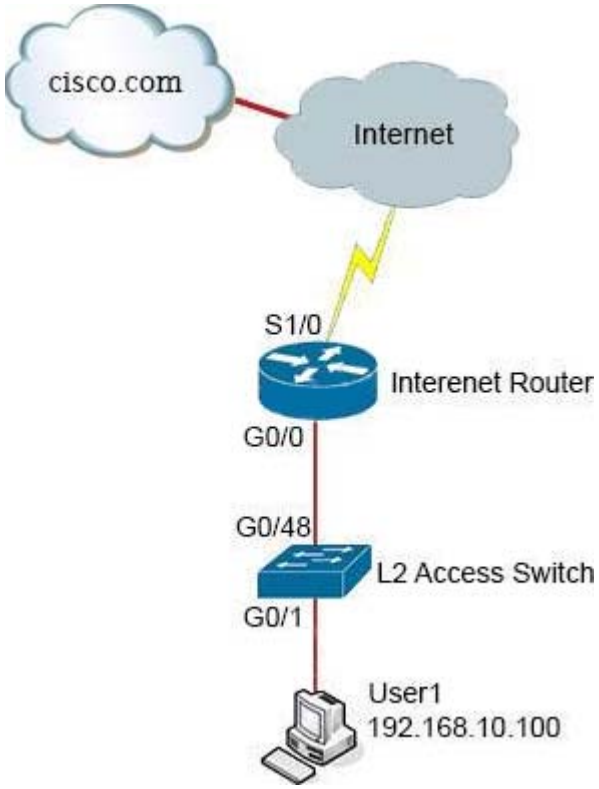
A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

Explanation:

https://community.cisco.com/t5/networking-documents/stateful-dhcpv6-relay-configuration-example/ta-p/3149338

150.A network administrator is tasked to permit http and https traffic only toward the internet from the User1 laptop to adhere to company's security policy. The administrator can still ping to www.cisco.com. Which interface should the access list 101 be applied to resolve this issue?




```
access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq 80
access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq 443
access-list 101 deny ip any any log
!
interface Serial1/0
 ip address 200.193.22.94 255.255.255.252
 ip access-group 101 in
```

A. Interface G0/48 in the incoming direction

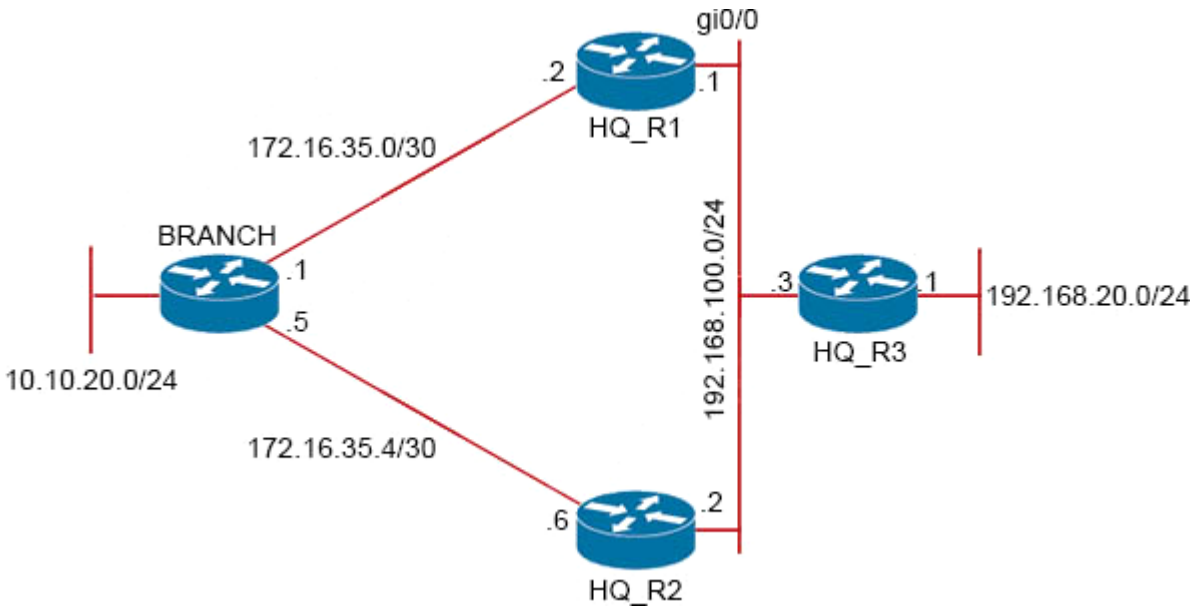
B. Interface G0/0 in the outgoing direction.

C. Interface S1/0 in the outgoing direction.

D. Interface G0/0 in the incoming direction.

Answer: D

151.Refer to Exhibit.




```
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.2 track 1
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.6 5
!
BRANCH(config)# ip sla 1
BRANCH(config-ip-sla)# icmp-echo 172.16.35.6
BRANCH(config-ip-sla)# timeout 200
BRANCH(config-ip-sla)# frequency 5
!
BRANCH(config)#ip sla schedule 1 life forever start-time now
!
BRANCH(config)# track 1 ip sla 1 reachability
```

Traffic from the branch network should route through HQ R1 unless the path is unavailable. An engineer tests this functionality by shutting down interface on the BRANCH router toward HQ_R1 router but 192.168.20.0/24 is no longer reachable from the branch router.

Which set of configurations resolves the issue?

A. HQ_R1(config)# ip sla responder

HQ_R1(config)# ip sla responder icmp-echo 172.16.35.2

B. BRANCH(config)# ip sla 1

BRANCH(config-ip-sla)# icmp-echo 172.16.35.1

C. HQ_R2(config)# ip sla responder

HQ_R2(config)# ip sla responder icmp-echo 172.16.35.5

D. BRANCH(config)# ip sla 1

BRANCH(config-ip-sla)# icmp-echo 172.16.35.2

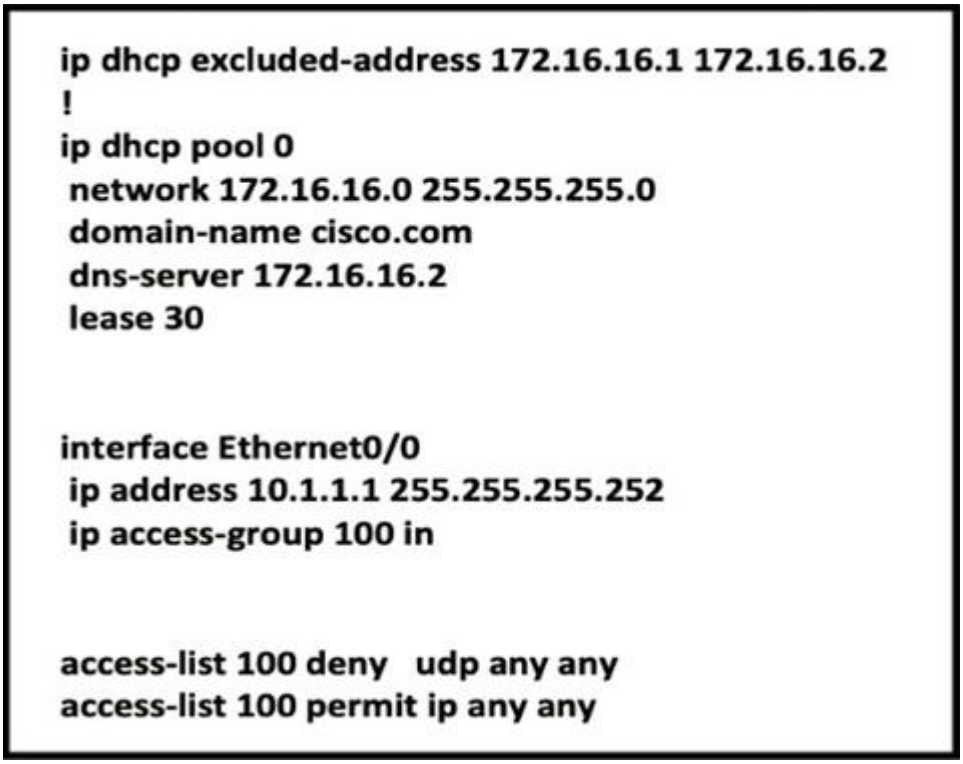
Answer: D

Explanation:

In the configuration above, the engineer has made a mistake as he was tracking 172.16.35.6 (the backup path) instead of tracking the main path (172.16.35.2). Therefore, when he shut down the main

path, the track 1 was still up so traffic still went through the main path -> it failed.
To fix this issue, we just need to correct the tracking interface of the main path.

152.Refer to Exhibit.



Which two configurations allow clients to get dynamic ip addresses assigned?
A. Configure access-list 100 permit udp any any eq 61 as the first line
B. Configure access-list 100 permit udp any any eq 86 as the first line
C. Configure access-list 100 permit udp any any eq 68 as the first line
D. Configure access-list 100 permit udp any any eq 69 as the first line
E. Configure access-list 100 permit udp any any eq 67 as the first line
Answer: CE
Explanation:
A DHCP server that receives a DHCPDISCOVER message may respond with a DHCPOFFER message on UDP port 68 (BootP client).
…
In the event that the DHCP server is not on the local subnet, the DHCP server will send the DHCPOFFER, as a unicast packet, on UDP port 67, back to the DHCP/BootPRelay Agent from which the DHCPDISCOVER came.
Reference: https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.html

153.Which Ipv6 first-hop security feature helps to minimize denial of service attacks?
A. IPv6 Router Advertisement Guard
B. IPv6 Destination Guard
C. DHCPv6 Guard

D. IPv6 MAC address filtering

Answer: B

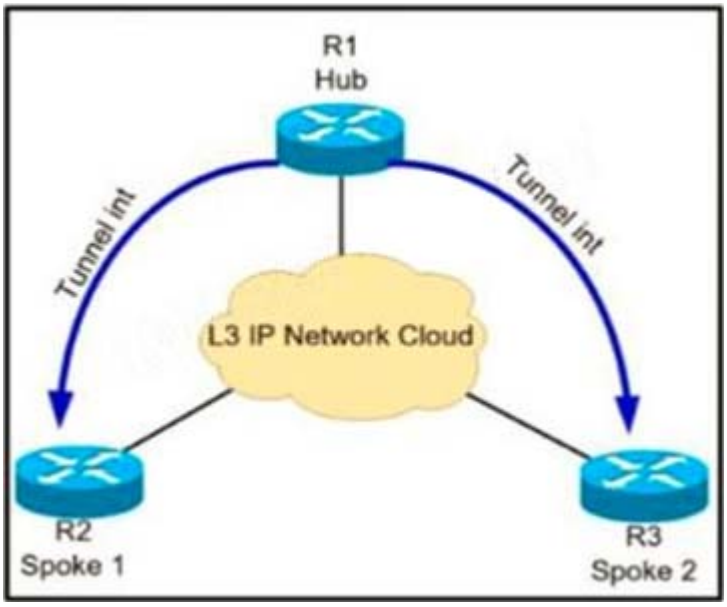
Explanation:

The Destination Guard feature helps in minimizing denial-of-service (DoS) attacks. It performs address resolutions only for those addresses that are active on the link,and requires the FHS binding table to be populated with the help of the IPv6 snooping feature.The feature enables the filtering of IPv6 traffic based on the destinationaddress, and blocks the NDP resolution for destination addresses that are not found in the binding table. By default, the policy drops traffic coming for an unknowndestination.

Reference:

https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book/IPv6_Security.pdf

154.Refer to Exhibit.



A network administrator has successfully configured DMVPN topology between a hub and two spoke routers.

Which two configuration commands should establish direct communications between spoke 1 and spoke 2 without going through the hub? (Choose two).

A. At the hub router, configure the ip nhrp shortcut command.

B. At the spoke routers, configure the ip nhrp spoke-tunnel command.

C. At the hub router, configure ip nhrp redirect the command

D. At the spoke routers, configure the ip nhrp shortcut command.

E. At the hub router, configure tne Ip nhrp spoke-tunnel command

Answer: C D

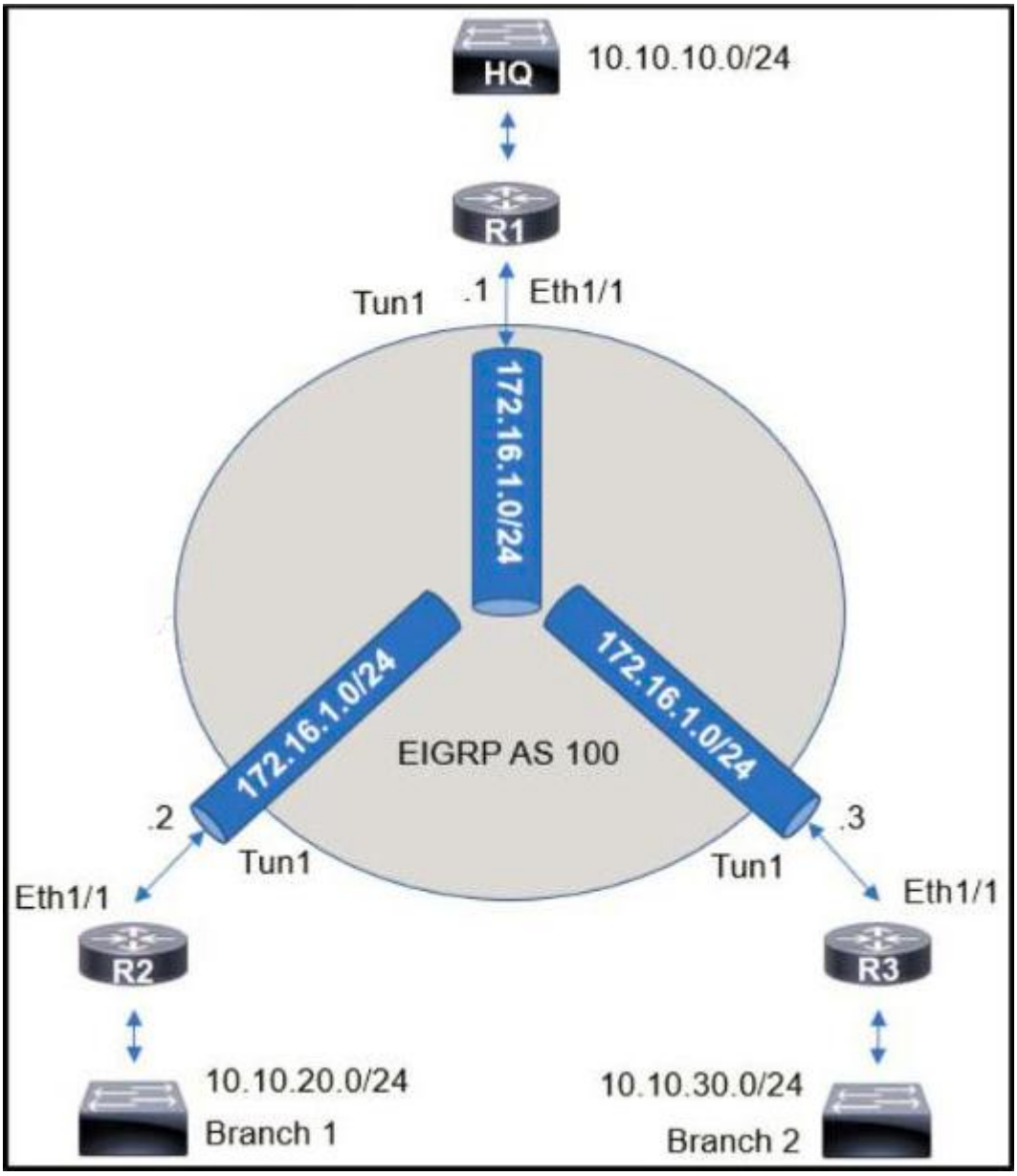
Explanation:

To configure Spoke to Spoke communication we can configure DMVPN Phase II or Phase III. But in Phase II, the first few packets would go through Hub. In order tototally ignore the hub, we have to use DMVPN Phase III:

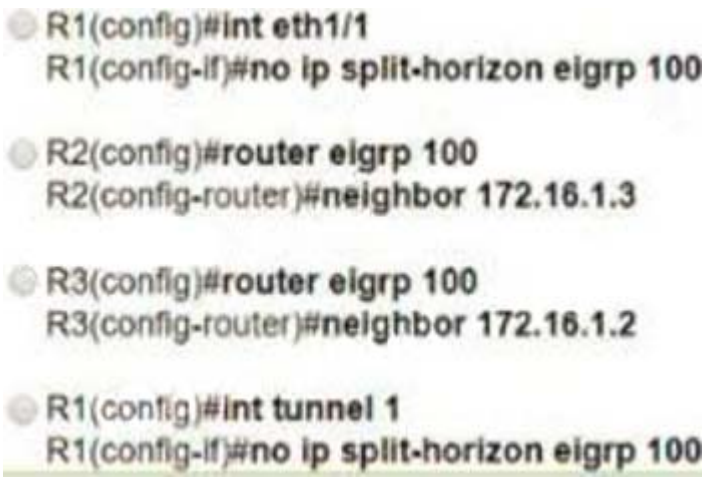
DMVPN Phase III is same as Phase 2 but removes some restrictions and complexities of Phase 2. Also allows greater variety of DMVPN network designs we use:

+ ip nhrp redirect in hub: tells the initiator spoke to look for a better path to the destination spoke than through the Hub. Upon receiving the NHRP redirect message thespokes communicate with each other over the hub and they have their NHRP replies for the NHRP Resolution Requests that they sent out.
+ ip nhrp shortcut in spokes: overwrite the CEF table on the spoke. It basically overrides the next-hop value for a remote spoke network from the default initial hubtunnel IP address to the NHRP resolved remote spoke tunnel IP address)

155.An engineer sets up a DMVPN connection to connect branch 1 and branch 2 to HQ branch 1 and branch 2 cannot communicate with each other.



Which change must be made to resolve this issue?



A. Option A
B. Option B
C. Option C
D. Option D
Answer: D
Explanation:
R1(config)#int tunnel 1
R1(config-if) no ip split-horizon eigrp 100

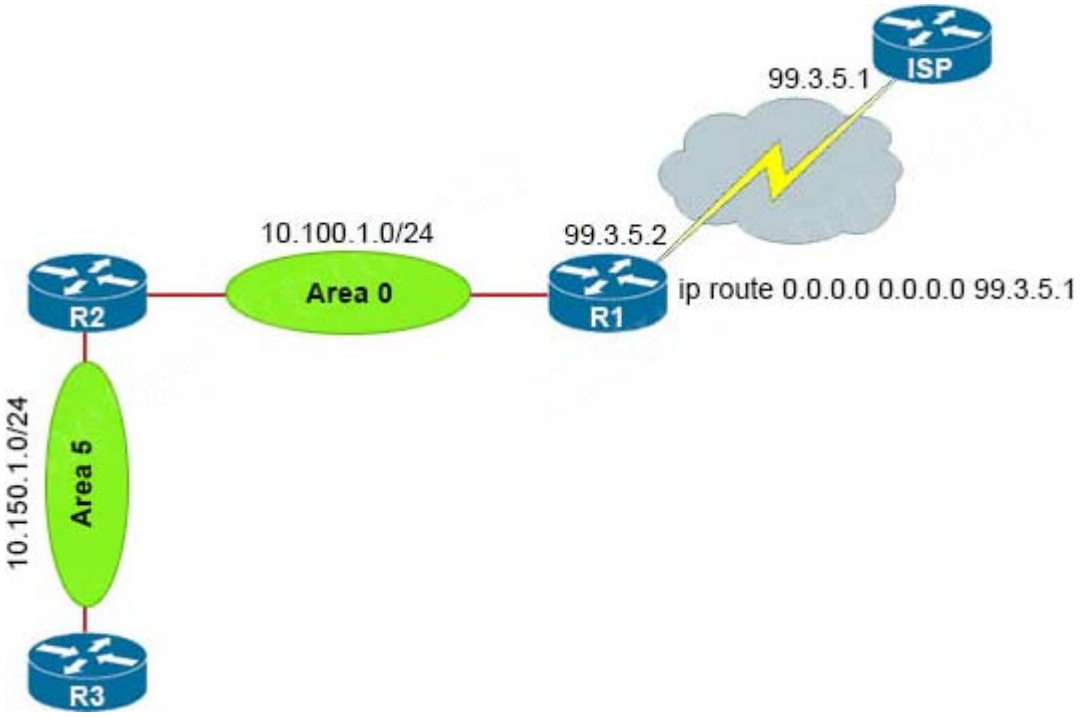
156.Refer to the exhibit.
access-list 1 permit 1.1.1.0 0.0.0.255
!
route-map FILTER1 deny 10
match ip address 1
!
router eigrp 1
distribute-list route-map FILTER1 in
Which action restores the routes from neighbors while still filtering 1.1.1.0/24?
A. Add a second line in the access list to permit any.
B. Modify the route map to permit the access list instead of deny it
C. Modify the access list to deny instead of permit it.
D. Add a second sequence in the route map permit 20
Answer: B

157.Which two components are needed for a service provider to utilize the LVPN MPLS application? (Choose two.)
A. The P routers must be configured for MP-iBGP toward the PE routers
B. The P routers must be configured with RSVP.
C. The PE routers must be configured for MP-iBGP with other PE routers
D. The PE routers must be configured for MP-eBGP to connect to CEs
E. The P and PE routers must be configured with LDP or RSVP
Answer: CE

Explanation:
MPLS Network Protocols
+ IGP: OSPF, EIGRP, IS-IS on core facing and core links+ RSVP and/or LDP on core and/or core facing links ->
+ MP-iBGP on PE devices (for MPLS services), MP-BGP: Multiprotocol Border Gateway Protocol, used for MPLS L3 VPN -> .
Reference: https://www.uio.no/studier/emner/matnat/ifi/IN3230/h19/kursmateriell/mpls-lecture.pdf

158.What are two characteristics of VRF instance? (Choose two.)
A. All VRFs share customers routing and CEF tables.
B. An interface must be associated to one VRF.
C. Each VRF has a different set of routing and CEF tables
D. It is defined by the VPN membership of a customer site attached to a P device.
E. A customer site can be associated to different VRFs
Answer: BC
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch_cef/configuration/xe-3s/isw-cef-xe-3s-book/isw-cef-basic-config.html
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-s/mp-l3-vpns-15-s-book/mp-bgp-mpls-vpn.pdf

159.Refer to the exhibit.



A network administrator redistributed the default static route into OSPF toward all internal routers to reach to Internet.
Which set of commands restores reachability to the Internet by internal routers?
A. router ospf 1

default-information originate
B. router ospf 1
network 0.0.0.0 0.0.0.0 area 0
C. router ospf 1
redistribute connected 0.0.0.0
D. router ospf 1
redistribute static subnets
Answer: A

160.Refer to the exhibit.

```
OSPF: Send DBD to 10.100.1.2 on GigabitEthernet0/1 seq 0x9E6 opt 0x52 flag 0x7 len 32
OSPF: Retransmitting DBD to 10.100.1.2 on GigabitEthernet0/1 [10]
OSPF: Send DBD to 10.100.1.2 on GigabitEthernet0/1 seq 0x9E6 opt 0x52 flag 0x7 len 32
OSPF: Retransmitting DBD to 10.100.1.2 on GigabitEthernet0/1 [11]
%OSPF-5-ADJCHG: Process 1, Nbr 10.100.1.2 on GigabitEthernet0/1 from EXSTART to
DOWN, Neighbor Down: Too many retransmissions
```

The OSPF neighbor relationship is not coming up.
What must be configured to restore OSPF neighbor adjacency?
A. OSPF on the remote router
B. matching hello timers
C. use router ID
D. matching MTU values
Answer: D

161.An engineer configured a DHCP server for Cisco IP phones to download its configuration from a TFTP server, but the IP phones failed to toad the configuration.
What must be configured to resolve the issue?
A. BOOTP port 67
B. DHCP option 66
C. BOOTP port 68
D. DHCP option 69
Answer: B
Explanation:

Command	Purpose

`dhcpd option 66 ascii server_name`
 	
Example:
`hostname(config)# dhcpd option 66 ascii exampleserver`
	Provides the IP address or name of a TFTP server for option 66.

DHCP options 3, 66, and 150 are used to configure Cisco IP Phones. Cisco IP Phones download their configuration from a TFTP server. When a Cisco IP Phone starts, ifit does not have both the IP address and TFTP server IP address preconfigured, it sends a request with option 150 or 66 to the DHCP server to obtain this information.

+ DHCP option 150 provides the IP addresses of a list of TFTP servers.
+ DHCP option 66 gives the IP address or the hostname of a single TFTP server.
Reference:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/basic_dhcp.pdf

162.Refer to the exhibit.

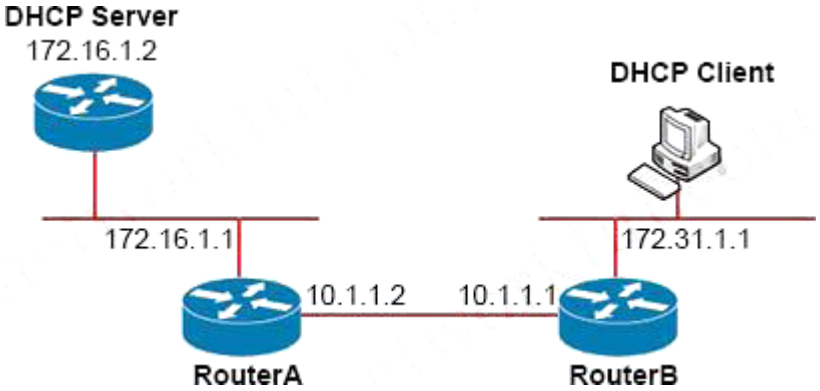
```
ipv6 unicast-routing
!
router ospfv3 4
 router-id 192.168.1.1
!
interface E0/0
 ipv6 enable
 ip address 10.1.1.1 255.255.255.0
 ospfv3 4 area 0 ipv4
 no shut
!
interface Loopback0
 ipv6 enable
 ipv4 172.16.1.1 255.255.255.0
 ospfv3 4 area 0 ipv4
```

The network administrator configured the branch router for IPv6 on the E 0/0 interface. The neighboring router is fully configured to meet requirements, but the neighbor relationship is not coming up.
Which action fixes the problem on the branch router to bring the IPv6 neighbors up?
A. Enable the IPv4 address family under the E 0/0 interface by using the address-family Ipv4 unicast command
B. Disable IPv6 on the E 0/0 interface using the no ipv6 enable command
C. Enable the IPv4 address family under the router ospfv3 4 process by using the address-family ipv4 unicast command
D. Disable OSPF for IPv4 using the no ospfv3 4 area 0 ipv4 command under the E 0/0 interface.
Answer: C
Explanation:
Once again, Cisco changed the IOS configuration commands required for OSPFv3 configuration. The new OSPFv3 configuration uses the “ospfv3” keyword instead ofthe earlier “ipv6 router ospf” routing process command and “ipv6 ospf” interface commands.
The Open Shortest Path First version 3 (OSPFv3) address families feature enables both IPv4 and IPv6 unicast traffic to be supported. With this feature, users may havetwo processes per interface, but only one process per address family (AF).

163.An engineer configured two routers connected to two different service providers using BGP with default attributes. One of the links is presenting high delay, which causes slowness in the network.

Which BGP attribute must the engineer configure to avoid using the high-delay ISP link if the second ISP link is up?
A. LOCAL_PREF
B. MED
C. WEIGHT
D. AS-PATH
Answer: A

164.Refer to the exhibit.



The DHCP client is unable to receive an IP address from the DHCP server
RouterB is configured as follows:

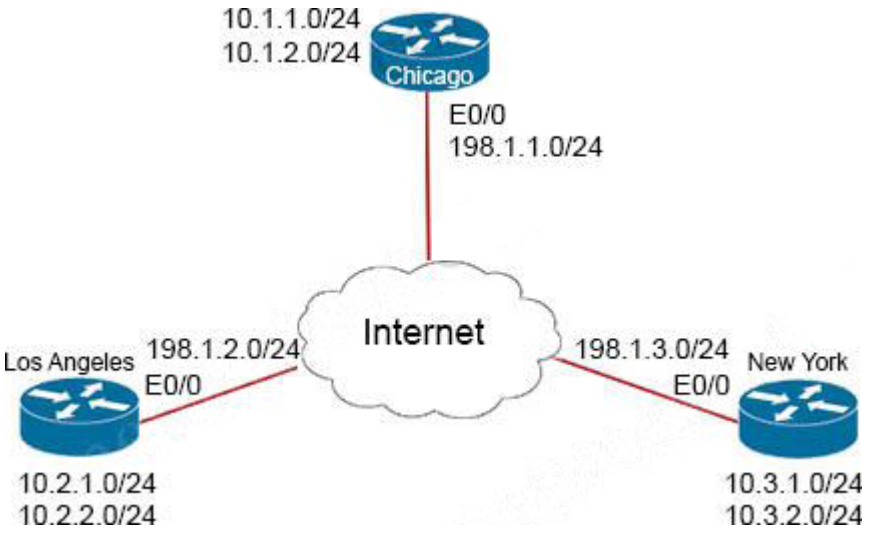
```
interface Fastethernet0/0
 description Client DHCP ID 43574645
 ip address 172.31.1.1 255.255.255.0
!
ip route 172.16.1.0 255.255.255.0 10.1.1.2
```

Which command is required on the fastethernet 0/0 interface of RouterB to resolve this issue?
A. RouterB(config-if)#Ip helper-address 172.31.1.1
B. RouterB(config-if)#Ip helper-address 255.255 255 255
C. RouterB(config-if)#Ip helper-address 172.16.1.1
D. RouterB(config-if)#Ip helper-address 172.16.1.2
Answer: D

165.What are two purposes of using IPv4 and VPNv4 address-family configurations in a Layer 3 MPLS VPN? (Choose two.)
A. The VPNv4 address is used to advertise the MPLS VPN label.
B. RD is prepended to the IPv4 route to make it unique.
C. MP-BGP is used to allow overlapping IPv4 addresses between customers to advertise through the network.
D. The IPv4 address is needed to tag the MPLS label.
E. The VPNv4 address consists of a 64-bit route distinguisher that is prepended to the IPv4 prefix.
Answer: BE

Explanation:
VPNv4 address consists of 64-bit Route Distinguisher (RD) prepended to IPv4 prefix. This is to make routes unique that are in different VRFs.

166.Refer to the exhibit.

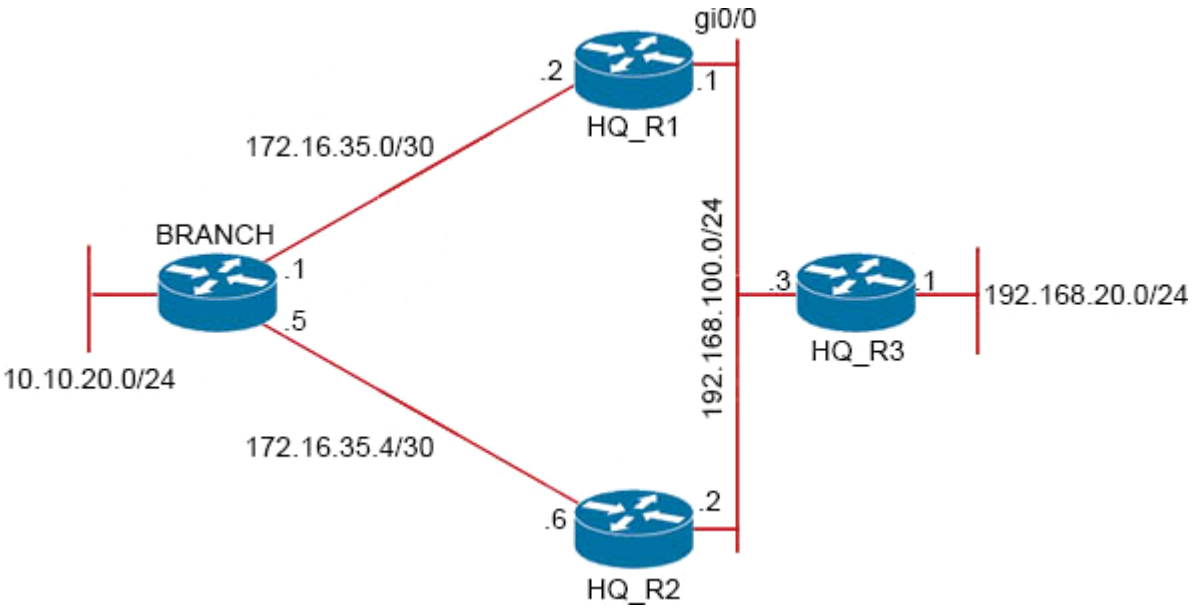



```
Chicago
interface Tunnel 1
 ip address 192.168.1.1255.255.255.0
 tunnel source E0/0
 tunnel mode gre multipoint
 ip nhrp network-id 1
 ip nhrp map multicast dynamic
 no ip next-hop-self eigrp 111
 tunnel protection ipsec profile IPSec-PROFILE
!
router eigrp 111
 network 192.168.1.0
 network 10.0.0.0
```

The Los Angeles and New York routers are receiving routes from Chicago but not from each other.
Which configuration fixes the issue?
A. Interface Tunnel1
no ip split-horizon eigrp 111
B. Interface Tunnel1
Ip next-hop-self elgrp 111
C. Interface Tunnel1
tunnel mode Ipsec Ipv4
D. Interface Tunnel1
tunnel protection ipsec profile IPSec-PROFILE
Answer: A

Explanation:
In this topology, Chicago router (Hub) will receive advertisements from Los Angeles (Spoke1) router on its tunnel interface. The problem here is that it also has a connection with New York (Spoke2) on that same tunnel interface. If we don't disable EIGRP split-horizon, then the Hub will not relay routes from Spoke1 to Spoke2 and the other way around. That is because it received those routes on interface Tunnel1 and therefore it cannot advertise back out that same interface (splithorizon rule). Therefore we must disable split-horizon on the Hub router to make sure the Spokes know about each other.

167.Refer to the exhibit.




```
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.2 track 1
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.6 5
!
BRANCH(config)# ip sla 1
BRANCH(config-ip-sla)# icmp-echo 172.16.35.6
BRANCH(config-ip-sla)# timeout 200
BRANCH(config-ip-sla)# frequency 5
!
BRANCH(config)#ip sla schedule 1 life forever start-time now
!
BRANCH(config)# track 1 ip sla 1 reachability
```

An engineer has successfully set up a floating static route from the BRANCH router to the HQ network using HQ_R1 as the primary default gateway. When the g0/0 goes down on HQ_R1, the branch network cannot reach the HQ network 192.168.20.0/24.
Which set of configurations resolves the issue?
A. HQ_R3(config)# ip sla responder
HQ_R3(config)# ip sla responder icmp-echo 172.16.35.1
B. BRANCH(config)# ip sla 1

BRANCH(config-ip-sla)# icmp-echo 192.168.100.2
C. HQ R3(config)# Ip sla responder
HQ R3(config)# Ip sla responder Icmp-echo 172.16.35.5
D. BRANCH(config)# Ip sla 1
BRANCH(config-ip-sta)# Icmp-echo 192.168.100.1
Answer: D

168.What are two functions of MPLS Layer 3 VPNs? (Choose two.)
A. LDP and BGP can be used for Pseudowire signaling.
B. It is used for transparent point-to-multipoint connectivity between Ethernet links/sites.
C. BGP is used for signaling customer VPNv4 routes between PE nodes.
D. A packet with node segment ID is forwarded along with shortest path to destination.
E. Customer traffic is encapsulated in a VPN label when it is forwarded in MPLS network.
Answer: CE
Explanation:
MPLS Layer-3 VPNs provide IP connectivity among CE sites
* MPLS VPNs enable full-mesh, hub-andspoke, and hybrid IP connectivity
* CE sites connect to the MPLS network via IP peering across PE-CE links
* MPLS Layer-3 VPNs are implemented via VRFs on PE edge nodes
* VRFs providing customer routing and forwarding segmentation
* BGP used for signaling customer VPN (VPNv4) routes between PE nodes
* To ensure traffic separation, customer traffic is encapsulated in an additional VPN label when forwarded in MPLS network
* Key applications are layer-3 business VPN services, enterprise network segmentation, and segmented layer-3 Data Center access
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKMPL-1100.pdf

169.When configuring Control Plane Policing on a router to protect it from malicious traffic, an engineer observes that the configured routing protocols start flapping on that device.
Which action in the Control Plane Policy prevents this problem in a production environment while achieving the security objective?
A. Set the conform-action and exceed-action to transmit initially to test the ACLs and transmit rates and apply the Control Plane Policy in the output direction
B. Set the conform-action and exceed-action to transmit initially to test the ACLs and transmit rates and apply the Control Plane Policy in the input direction
C. Set the conform-action to transmit and exceed-action to drop to test the ACLs and transmit rates and apply the Control Plane Policy m the input direction
D. Set the conform-action to transmit and exceed-action to drop to test the ACLs and transmit rates and apply the Control Plane Policy m the output direction
Answer: B

170.Refer to the exhibit.

```
ip prefix-list DefaultRouteOnly seq 5 deny 0.0.0.0/0 le 32
ip prefix-list DefaultRouteOnly seq 10 permit 0.0.0.0/0

router eigrp ccnp
 address-family ipv4 unicast autonomous-system 1
  topology base
   distribute-list prefix DefaultRouteOnly out Tunnel0
```

The administrator configured route advertisement to a remote low resources router to use only the default route to reach any network but failed.

Which action resolves this issue?

A. Change the direction of the distribute-list command from out to in.

B. Remove the line with the sequence number 5 from the prefix list.

C. Remove the prefix keyword from the distribute-list command.

D. Remove the line with the sequence number 10 from the prefix list.

Answer: B

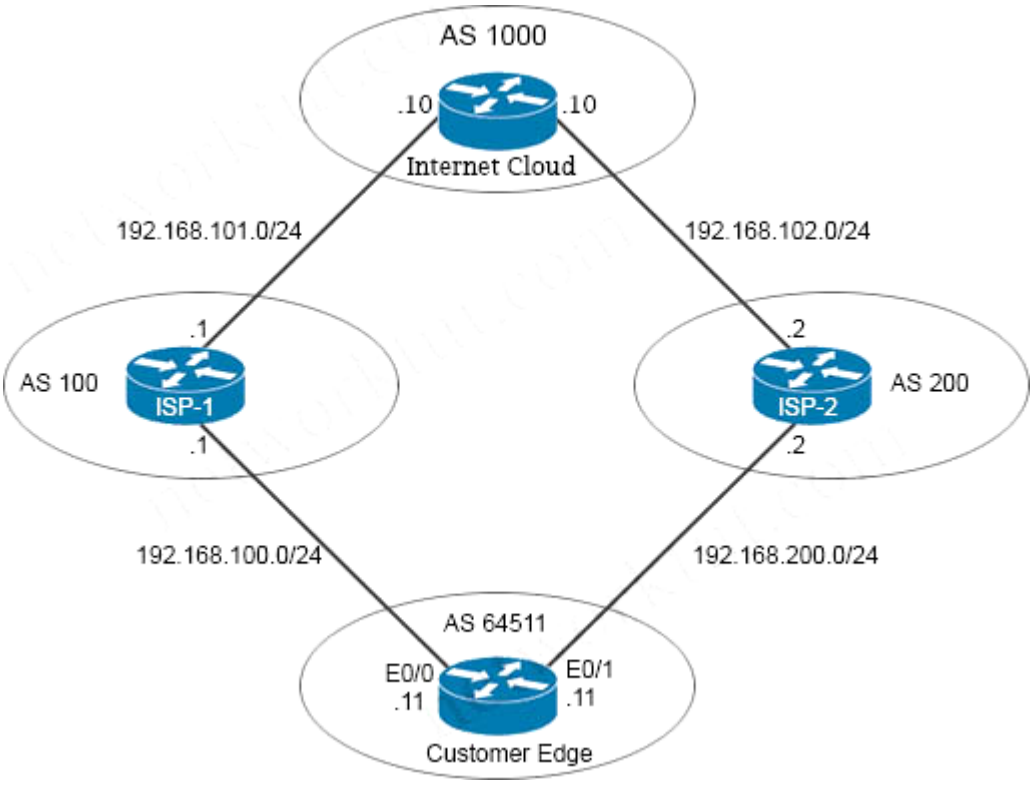
171.Refer to the exhibit.

```
config t
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow exporter EXPORTER-1
 destination 172.16.10.2
 transport udp 2055
 exit
!
flow monitor FLOW-MONITOR-1
 exporter EXPORTER-1
 record v4_r1
 exit
!
flow monitor v4_r1
!
ip cef
!
interface Ethernet0/0.1
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor v4_r1 input
!
```

The remote server is failing to receive the NetFlow data.
Which action resolves the issue?
A. Modify the flow transport command transport udp 2055 to move under flow monitor profile.
B. Modify the interlace command to Ip flow monitor FLOW-MONITOR-1 Input.
C. Modify the udp port under flow exporter profile to Ip transport udp 4739.
D. Modify the flow record command record v4_r1 to move under flow exporter profile.
Answer: B
Explanation:
From the exhibit we see there are two flow monitors: the first one “FLOW-MONITOR-1” has been configured correctly but the second one “v4_r1” was left empty andinterface E0/0.1 is using it. So the remote server does not receive any NetFlow data.

172.A DMVPN single hub topology is using IPsec + mGRE with OSPF.
What should be configured on the hub to ensure it will be the designated router?
A. tunnel interface of the hub with ip nhrp ospf dr
B. OSPF priority to 0
C. route map to set the metrics of learned routes to 110
D. OSPF priority greater than 1
Answer: D
Explanation:
By default, the priority is 1 on all routers so we can set the OSPF priority of the hub to a value which is greater than 1 to make sure it would become the DR.

173.Refer to the exhibit.



The network administrator has configured the Customer Edge router (AS 64511) to send only

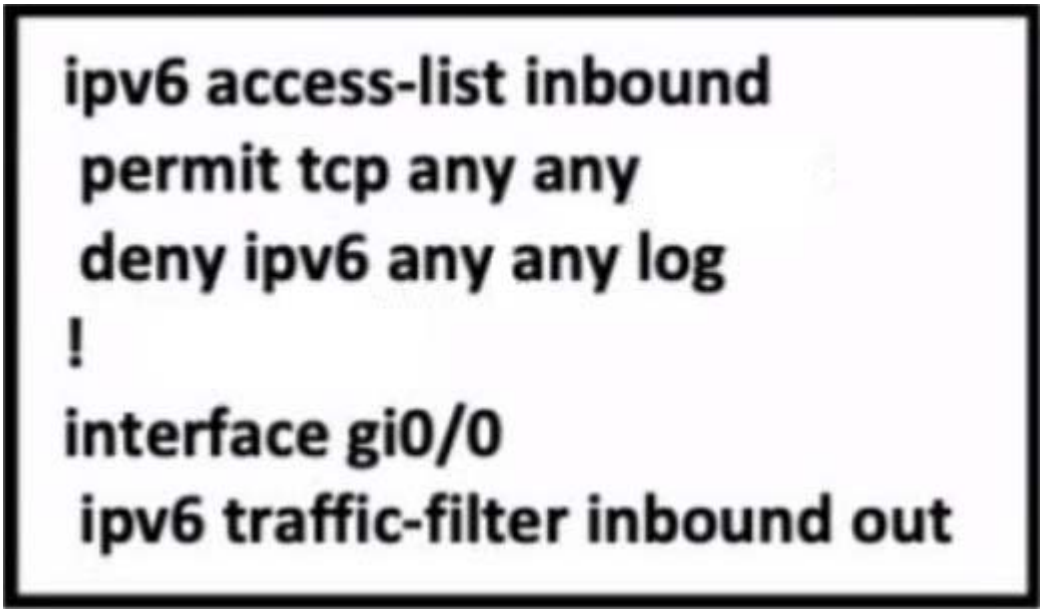
summarized routes toward ISP-1 (AS 100) and ISP-2 (AS 200).
router bgp 64511
network 172.16.20.0 mask 255.255.255.0
network 172.16.21.0 mask 255.255.255.0
network 172.16.22.0 mask 255.255.255.0
network 172.16.23.0 mask 255.255.255.0
aggregate-address 172.16.20.0 255.255.252.0
After this configuration. ISP-1 and ISP-2 continue to receive the specific routes and the summary route.
Which configuration resolves the issue?
A. router bgp 64511
aggregate-address 172.16.20.0 255.255.252.0 summary-only
B. router bgp 64511
neighbor 192.168.100.1 summary-only
neighbor 192.168.200.2 summary-only
C. interface E 0/0
ip bgp suppress-map BLOCK_SPECIFIC
!
interface E 0/1
ip bgp suppress-map BLOCK_SPECIFIC
!
ip prefix-list PL_BLOCK_SPECIFIC
permit 172.16.20.0/22 ge 24
!
route-map BLOCK_SPECIFIC permit 10
match ip address prefix-list PL_BLOCK_SPECIFIC
D. ip prefix-list PL_BLOCK_SPECIFIC
deny 172.16.20.0/22 ge 22
ip prefix-list PL BLOCK SPECIFIC
permit 172.16.20.0/22
!
route-map BLOCK_SPECIFIC permit 10
match ip address prefix-list PL_BLOCK_SPECIFIC
!
router bgp 64511
aggregate-address 172.16.20.0 255 255.252.0 suppress-map BLOCKSPECIFIC
Answer: A
Explanation:
When the aggregate-address command is used within BGP routing, the aggregated address is advertised, along with the more specific routes. The exception to this rule is through the use of the summary-only command. The “summary-only” keyword suppresses the more specific routes and announces only the summarized route.

174.What are two MPLS label characteristics? (Choose two.)
A. The label edge router swaps labels on the received packets.

B. Labels are imposed in packets after the Layer 3 header.
C. LDP uses TCP for reliable delivery of information.
D. An MPLS label is a short identifier that identifies a forwarding equivalence class.
E. A maximum of two labels can be imposed on an MPLS packet.
Answer: CD
Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/4649-mpls-faq-4649.html

175.In which two ways does the IPv6 First-Hop Security Binding Table operate? (Choose two.)
A. by IPv6 routing protocols to securely build neighborships without the need of authentication
B. by the recovery mechanism to recover the binding table in the event of a device reboot
C. by IPv6 HSRP to make sure neighbors are authenticated before being used as gateways
D. by various IPv6 guard features to validate the data link layer address
E. by storing hashed keys for IPsec tunnels for the built-in IPsec features
Answer: B, D
Explanation:
Overview of the IPv6 First-Hop Security Binding Table
A database table of IPv6 neighbors connected to the device is created from information sources such as NDP snooping. This database, or binding table, is used by variousIPv6 guard features to validate the link-layer address (LLA), the IPv4 or IPv6 address, and the prefix binding of the neighbors to prevent spoofing and redirect attacks.
IPv6 First-Hop Security Binding Table Recovery Mechanism. The IPv6 first-hop security binding table recovery mechanism enables the binding table to recover in the event of a device reboot.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-s/ip6-fhs-bind-table.html

176.Refer to the exhibit.



A network administrator configured an IPv6 access list to allow TCP return traffic only, but it is not

working as expected.

Which changes resolve this issue?

A)

```
ipv6 access-list inbound
 permit tcp any any syn
 deny ipv6 any any log
!
interface gi0/0
 ipv6 traffic-filter inbound in
```

B)

```
ipv6 access-list inbound
 permit tcp any any established
 deny ipv6 any any log
!
interface gi0/0
 ipv6 traffic-filter inbound out
```

C)

```
ipv6 access-list inbound
 permit tcp any any established
 deny ipv6 any any log
!
interface gi0/0
 ipv6 traffic-filter inbound in
```

D)

```
ipv6 access-list inbound
 permit tcp any any syn
 deny ipv6 any any log
!
interface gi0/0
 ipv6 traffic-filter inbound out
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

177.Refer to the exhibit.

Configuration output:

```
clock timezone PST -8
clock summer-time PDT recurring
service timestamps debug datetime
service timestamps log datetime
logging buffered 16000 debugging
ntp clock-period 17178272
ntp server 161.181.92.152
```

Debug output:

```
router#show clock
14:12:26:312 PDT Thu Apr 27 2019
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#exit

router#
Apr 27 21:12:28: %SYS-5-CONFIG_I: Configured from console by vty0
```

A network administrator configured NTP on a Cisco router to get synchronized time for system and logs from a unified time source. The configuration did not work as desired.
Which service must be enabled to resolve the issue?
A. Enter the service timestamps log datetime localtime global command.
B. Enter the service timestamps log datetime synchronize global command.
C. Enter the service timestamps log datetime console global command.
D. Enter the service timestamps log datetime clock-period global command
Answer: A
Explanation:
If a router is configured to get the time from a Network Time Protocol (NTP) server, the times in the router's log entries may be different from the time on the systemclock if the [localtime] option is not in the service timestamps log command. To solve this issue, add the [localtime] option to the service timestamps log command. Thetimes should now be synchronized between the system clock and the log message timestamps.
Reference: https://community.cisco.com/t5/networking-documents/router-log-timestamp-entries-are-different-from-the-system-clock/ta-p/3132258

178.Refer to the exhibit.


```
ip access list extended EGRESS2
 10 deny ip any any
!
interface GigabitEthernet0/0
 ip address 209.165.201.1 255.255.255.0
 ip access-group EGRESS2 out
 duplex auto
 speed auto
 media-type rj45
 ipv6 address 2001:DB8::1/64
!
line vty 0 4
 no login
 transport input telnet
```

```
ipv6 access-list INGRESS
 permit ipv6 2001:DB8::/64 any sequence 10
 deny ipv6 2001:DB8::/32 any sequence 20
!
interface GigabitEthernet0/0
 ip address 209.165.201.25 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 ipv6 address autoconfig
 ipv6 nd autoconfig default-route
 ipv6 nd cache expire 60
 ipv6 nd ra suppress
 ipv6 traffic-fiter INGRESS in
 ipv6 nd ra suppress
```

The engineer configured and connected Router2 to Router1. The link came up but could not establish a Telnet connection to Router1 IPv6 address of 2001:DB8::1.

Which configuration allows Router2 to establish a Telnet connection to Router1?

A. jpv6 unicast-routing

B. permit ICMPv6 on access list INGRESS for Router2 to obtain IPv6 address

C. permit ip any any on access list EGRESS2 on Router1

D. IPv6 address on GigabitEthernet0/0

Answer: D

Explanation:

----------R1----------

interface Ethernet0/0

ip address 209.165.201.1 255.255.255.0

ip access-group EGRESS2 out

ipv6 address 2001:DB8::1/64

end

----------R2----------

interface Ethernet0/0

ip address 209.165.201.25 255.255.255.0

ipv6 address 2001:DB8::2/64

ipv6 address autoconfig

ipv6 nd autoconfig default-route

ipv6 nd cache expire 60

ipv6 nd ra suppress

ipv6 traffic-filter INGRESS in

end

IOU_Router2#telnet 2001:DB8::1

Trying 2001:DB8::1 ... Open

IOU_Router1>

179.Refer to the exhibits.

Filtered

```
00:00:35: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:36: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:36: %LINK-3-UPPOWN: Interface GigabitEthernet0/2, changed state to up
```

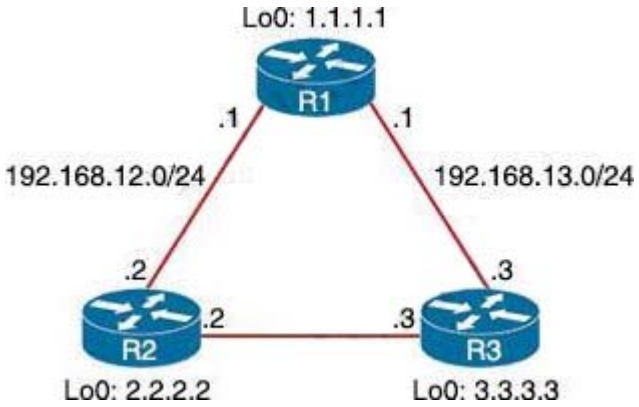
Desired

```
00:00:35: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:36: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:36: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:37: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:37: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down
2 *Jun 1 18:46:11: %SYS-6-CONFIG_I: Configured from console by vty2
```

An engineer filtered messages based on severity to minimize log messages. After applying the filter, the engineer noticed that it filtered required messages as well.
Which action must the engineer take to resolve the issue?
A. Configure syslog level 2.
B. Configure syslog level 3.
C. Configure syslog level 4.
D. Configure syslog level 5.
Answer: D

180.An engineer configured policy-based routing for a destination IP address that does not exist in the routing table.
How is the packet treated through the policy for configuring the set ip default next-hop command?
A. Packets are not forwarded to the specific next hop.
B. Packets are forwarded based on the routing table.
C. Packets are forwarded based on a static route.
D. Packets are forwarded to the specific next hop.
Answer: D
Explanation:
The set ip default next-hop command verifies the existence of the destination IP address in the routing table, and…+ if the destination IP address exists, the command does not policy route the packet, but forwards the packet based on the routing table.+ if the destination IP address does not exist, the command policy routes the packet by sending it to the specified next hop.
Reference: https://www.cisco.com/c/en/us/support/docs/ip/ip-routed-protocols/47121-pbr-cmds-ce.html

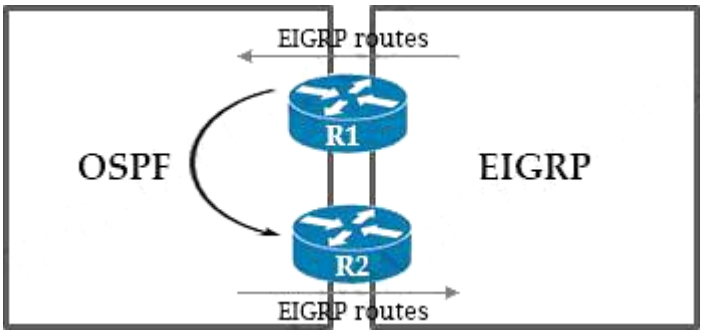
181.Refer to the exhibit.




```
R2#show ip protocols | include eigrp|Maximum
Routing Protocol is "eigrp 1"
 Maximum path: 4
 Maximum hopcount 100
 Maximum metric variance 1

R2#show ip eiqrp topology 192.168.13.0/24
EIGRP-IPv4 Topology Entry for AS(1)/ID(2.2.2.2) for 192.168.13.0/24
 State is Passive, Query origin flag is 1, 1 Successor(s), FD is 1075200
 Descriptor Blocks:
 192.168.23.3 (FastEthernet0/1), from 192.168.23.3, Send flag is 0x0
  Composite metric is (1075200/281600), route is Internal
  Vector metric:
   Minimum bandwidth is 2500 Kbit
   Total delay is 2000 microseconds
   Reliability is 255/255
   Load is 255/255
   Minimum MTU is 1500
   Hop count is 1
   Originating router is 3.3.3.3
 192.168.12.1 (FastEthernet0/0), from 192.168.12.1, Send flag is 0x0
   Composite metric is (2611200/281600), route is Internal
   Vector metric
    Minimum bandwidth is 1000 Kbit
        Total delay is 2000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
        Originating router is 1.1.1.1

R2#show ip route 192.168.13.0
Routing entry for 192.168.13.0/24
 Known via "eigrp 1", distance 90, metric 1075200, type internal
 Redistributing via eigrp 1
 Last update from 192.168.23.3 on FastEthernet0/1, 00:00:57 ago
 Routing Descriptor Blocks:
 * 192.168.23.3, from 192.168.23.3, 00:00:57 ago, via FastEthernet0/1
  Route metric a 1075200, traffic share count is 1
  Total delay is 2000 microseconds, minimum bandwidth is 2500 Kbit
  Reliability 255/255, minimum MTU 1500 bytes
  Loading 255/255, Hops 1
```

R2 has two paths to reach 192.168.13.0/24. but traffic is sent only through R3.
Which action allows traffic to use both paths?
A. Configure the bandwidth 2000 command under interface FastEthernet0/0 on R2.
B. Configure the variance 4 command under the EIGRP process on R2.
C. Configure the delay 1 command under interface FastEthernet0/0 on R2.
D. Configure the variance 2 command under the EIGRP process on R2
Answer: B
Explanation:
From the output of the “show ip eigrp topology …” command, we notice network 192.168.13.0/24 was learned via two routes:
+ From 192.168.23.3 (R3) with FD = 1075200 and AD = 281600
+ From 192.168.12.1 (R1) with FD = 2611200 and AD = 281600
From the output of the “show ip route …” command, we learned that the best (and chosen) path is via 192.168.23.3 (R3).
To use both paths (called unequal cost load balancing) with EIGRP, the second path via R1 must satisfy the feasibility condition. The feasibility condition states that, the Advertised Distance (AD) of a route must be lower than the feasible distance of the current successor route.
In this case, the second path satisfies the feasible condition as its AD (281600) is smaller than the FD (1075200) of the best path. Therefore we can configure loadbalancing with “variance” command.
In other words, EIGRP will install all paths with metric < variance * best_metric into the local routing table, provided that it meets the feasibility condition to preventrouting loop. Therefore we can calculate the variance > metric / best_metric = 2611200 / 1075200 =2.4.
So with a variance greater than 2 (and must be an integer), we can load balance traffic to network 192.168.13.0/24.

182.Refer to the exhibit.



A network administrator configured mutual redistribution on R1 and R2 routers, which caused instability in the network.
Which action resolves the issue?
A. Set a tag in the route map when redistributing EIGRP into OSPF on R1. and match the same tag on R2 to deny when redistributing OSPF into EIGRP.
B. Set a tag in the route map when redistributing EIGRP into OSPF on R1. and match the same tag on R2 to allow when redistributing OSPF into EIGRP.
C. Advertise summary routes of EIGRP to OSPF and deny specific EIGRP routes when redistributing into OSPF.
D. Apply a prefix list of EIGRP network routes in OSPF domain on R1 to propagate back into the EIGRP

routing domain.
Answer: A

183.Refer to the exhibit.
R1

```
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
interface FastEthernet0/0
 ip address 192.168.12.1 255.255.255.0
router eigrp 100
 no auto-summary
 network 192.168.12.0
 network 172.16.0.0
 neighbor 192.168.12.2
```

R2

```
interface Loopback0
 ip address 172.16.2.2 255.255.255.255
interface FastEthernet0/0
 ip address 192.168.12.2 255.255.255.0
router eigrp 100
 network 192.168.12.0
 network 172.16.0.0
 neighbor 192.168.12.1
 passive-interface FastEthernet0/0
```

R1 and R2 cannot establish an EIGRP adjacency.
Which action establishes EIGRP adjacency?
A. Remove the current autonomous system number on one of the routers and change to a different value.
B. Remove the passive-interface command from the R2 configuration so that it matches the R1 configuration.
C. Add the no auto-summary command to the R2 configuration so that it matches the R1 configuration.
D. Add the passive-interface command to the R1 configuration so that it matches the R2 configuration.
Answer: B

184.When configuring Control Plane Policing on a router to protect it from malicious traffic, an engineer observes that the configured routing protocols start flapping on that device.
Which action in the Control Plane Policy prevents this problem in a production environment while achieving the security objective?
A. Set the conform-action and exceed-action to transmit initially to test the ACLs and transmit rates and apply the Control Plane Policy in the output direction
B. Set the conform-action and exceed-action to transmit initially to test the ACLs and transmit rates and apply the Control Plane Policy in the input direction
C. Set the conform-action to transmit and exceed-action to drop to test the ACLs and transmit rates and apply the Control Plane Policy m the input direction
D. Set the conform-action to transmit and exceed-action to drop to test the ACLs and transmit rates and

apply the Control Plane Policy m the output direction
Answer: B

185.Refer to Exhibit.

```
ipv6 unicast-routing
!
router ospfv3 4
 router-id 192.168.1.1
!
interface E0/0
 ipv6 enable
 ip address 10.1.1.1 255.255.255.0
 ospfv3 4 area 0 ipv4
 no shut
!
interface Loopback0
 ipv6 enable
 ipv4 172.16.1.1 255.255.255.0
 ospfv3 4 area 0 ipv4
```

The network administrator configured the branch router for IPv6 on the E0/0 interface. The neighboring router is fully configured to meet requirements, but the neighbor relationship is not coming up.
Which action fixes the problem on the branch router to bring the IPv6 neighbors up?
A. Enable the IPv4 address family under the router ospfv3 4 process by using the address-family ipv4 unicast command
B. Disable IPv6 on the E0/0 interface using the no ipv6 enable command
C. Enable the IPv4 address family under the E0/0 interface by using the address-family ipv4 unicast command
D. Disable OSPF for IPv4 using the no ospfv3 4 area 0 ipv4 command under the E0/0 interface
Answer: A
Explanation:
Once again, Cisco changed the IOS configuration commands required for OSPFv3 configuration. The new OSPFv3 configuration uses the “ospfv3” keyword instead of the earlier “ipv6 router ospf” routing process command and “ipv6 ospf” interface commands.
The Open Shortest Path First version 3 (OSPFv3) address families feature enables both IPv4 and IPv6 unicast traffic to be supported. With this feature, users may have two processes per interface, but only one process per address family (AF).

186.An engineer is troubleshooting on the console session of a router and turns on multiple debug commands. The console screen is filled with scrolling debug messages that none of the commands can be verified if entered correctly or display any output.
Which action allows the engineer to see entered console commands while still continuing the analysis of the debug messages?

A. Configure the logging synchronous command
B. Configure the no logging console debugging command globally
C. Configure the logging synchronous level all command
D. Configure the term no mon command globally
Answer: A
Explanation:
Let's see how the "logging synchronous" command affect the typing command:
Without this command, a message may pop up and you may not know what you typed if that message is too long. When trying to erase (backspace) your command, you realize you are erasing the message instead.

```
NVbos2811-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
NVbos2811-1(config)#^Z
NVbos2811-1#sh
Jan 18 16:38:02: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (10.0.1.111
```

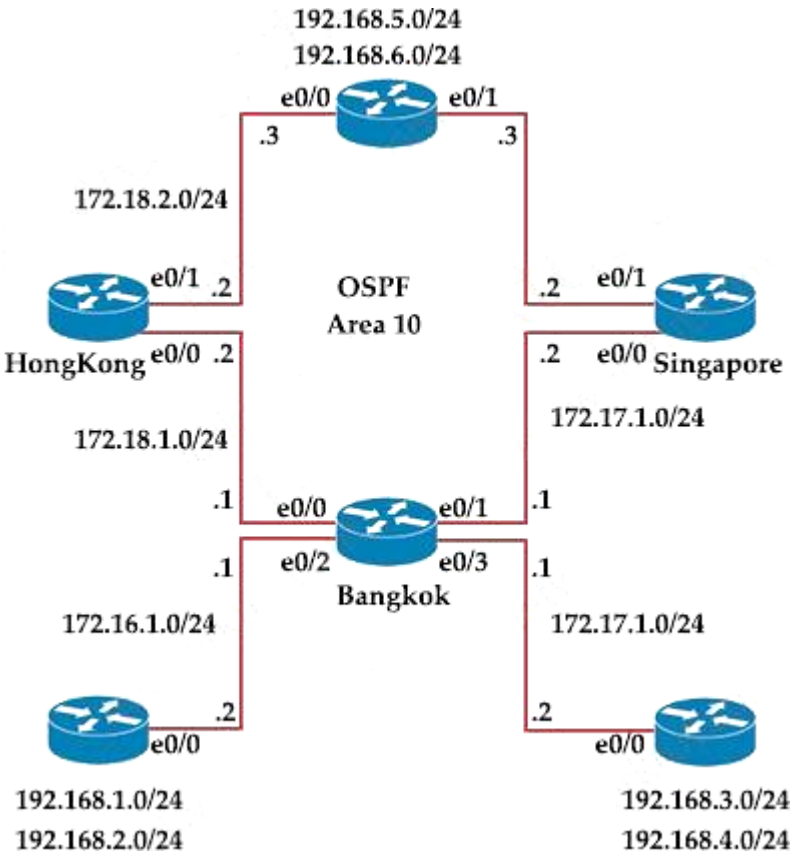
With this command enabled, when a message pops up you will be put to a new line with your typing command which is very

```
NVbos2811-1(config)#line con 0
NVbos2811-1(config-line)#logging synch
NVbos2811-1(config-line)#line vty 0 4
NVbos2811-1(config-line)#logging synchr
NVbos2811-1(config-line)#logging synchronous
NVbos2811-1(config-line)#^Z
NVbos2811-1#sh ip
Jan 18 16:39:33: %SYS-5-CONFIG_I: Configured from console by admin
NVbos2811-1#sh ip
```

187.An engineer must configure a Cisco router to initiate secure connections from the router to other devices in the network but kept failing.
Which two actions resolve the issue? (Choose two.)
A. Configure a source port for the SSH connection to initiate
B. Configure a TACACS+ server and enable it
C. Configure transport input ssh command on the console
D. Configure a domain name
E. Configure a crypto key to be generated
Answer: D E
Explanation:
Follow these guidelines when configuring the switch as an SSH server or SSH client:
+ An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.
+ If the SSH server is running on a stack master and the stack master fails, the new stack master uses the RSA key pair generated by the previous stack master
+ If you get CLI error messages after entering the crypto key generate rsa global configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the crypto key generate rsa command.
+ When generating the RSA key pair, the message No host name specified might appear. If it does, you must configure a hostname by using the hostname global configuration command.

+ When generating the RSA key pair, the message No domain specified might appear. If it does, you must configure an IP domain name by using the ip domain-nameglobal configuration command.
+ When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.
Reference:
https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_01100

188.Exhibit:



Bangkok is using ECMP to reach to the 192.168.5.0/24 network. The administrator must configure Bangkok in such a way that Telnet traffic from 192.168.3.0/24 and192.168.4.0/24 networks uses the HongKong router as the preferred router.
Which set of configurations accomplishes this task?
A. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255
access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255
!
route-map PBR1 permit 10
match ip address 101
set ip next-hop 172.18.1.2
interface Ethernet0/3
ip policy route-map PBR1
B. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23
access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23

!
route-map PBR1 permit 10
match ip address 101
set ip next-hop 172.18.1.2
interface Ethernet0/1
ip policy route-map PBR1
C. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23
access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23
!
route-map PBR1 permit 10
match ip address 101
set ip next-hop 172.18.1.2
!
interface Ethernet0/3
ip policy route-map PBR1
D. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255
access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255
!
route-map PBR1 permit 10
match ip address 101
set ip next-hop 172.18.1.2
!
interface Ethernet0/1
ip policy route-map PBR1
Answer: C
Explanation:
We need to use Policy Based Routing (PBR) here on Bangkok router to match the traffic from 192.168.3.0/24 & 192.168.4.0/24 and “set ip next-hop” to HongKong router (172.18.1.2 in this case).
Note: Please notice that we have to apply the PBR on incoming interface e0/3 to receive traffic from 192.168.3.0/24 and 192.168.4.0/24.

189.Exhibit:

```
11:27:07.532: AAA/BIND (00000055): Bind i/
11:27:07.532: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
11:27:07.532: TPLUS: Queuing AAA Authentication request 85 for processing
11:27:07.532: TPLUS (00000055) login timer started 1020 sec timeout
11:27:07.532: TPLUS: processing authentication start request id 85
11:27:07.532: TPLUS: Authentication start packet created for 85()
11:27:07.532: TPLUS: Using server 10.106.60.182
11:27:07.532: TPLUS (00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
11:27:07.532: TPLUS (00000055)/0/NB_WAIT: socket event 2
11:27:07.532: TPLUS (00000055)/0/NB_WAIT: wrote entire 38 bytes request
11:27:07.532: TPLUS (00000055)/0/READ: socket event 1
11:27:07.532: TPLUS (00000055)/0/READ: Would block while reading
11:27:07.532: TPLUS (00000055)/0/READ: socket event 1
11:27:07.532: TPLUS (00000055)/0/READ: react entire 12 header bytes (expect 6 bytes data)
13:27:07.532: TPLUS (00000055)/0/READ: socket event 1
11:27:07.532: TPLUS (00000055)/0/READ: read entire 18 bytes response
11:27:07.532: TPLUS (00000055)/0/225FE2DC: Processing the reply packet
11:27:07.532: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
11:27:07.532: TPLUS: Invalid AUTHEN packet (check keys).
```

Which action resolves the authentication problem?

A. Configure the user name on the TACACS+ server

B. Configure the UDP port 1812 to be allowed on the TACACS+ server

C. Configure the TCP port 49 to be reachable by the router

D. Configure the same password between the TACACS+ server and router.

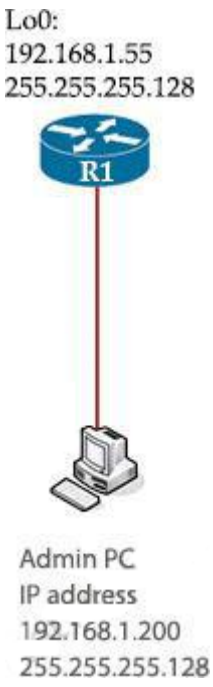
Answer: D

Explanation:

From the last line of the output, we notice that the result was “Invalid AUTHEN packet”. Therefore something went wrong with the username or password.

Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/200467-Troubleshoot-TACACS-Authentication-Issue.html

190.Refer to the exhibit.




```
aaa new-model
!
aaa authentication login default line enable
aaa authorization commands 15 default local
aaa authorization network default local
!
username admin privilege 15 password cisco123!
!
ip ssh version 2
!

access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 22
access-list 101 permit tcp 192.168.5.0 0.0.0.255 any range 22 smtp
!
line vty 0 4
access-class 101 in
password cisco
transport input all
!
line vty 5 15
access-class 101 in
password cisco
transport input all
```

The administrator successfully logs into R1 but cannot access privileged mode commands.

What should be configured to resolve the issue?

A. aaa authorization reverse-access

B. secret cisco123! at the end of the username command instead of password cisco123!
C. matching password on vty lines as cisco123!
D. enable secret or enable password commands to enter into privileged mode
Answer: D

191.DRAG DROP
Drag and drop the MPLS concepts from the left onto the descriptions on the right.

label edge router	allows an LSR to remove the label before forwarding the packet
label switch router	accepts unlabeled packets and imposes labels
forwarding equivalence class	group of packets that are forwarded in the same manner
penultimate hop popping	receives labeled packets and swaps labels

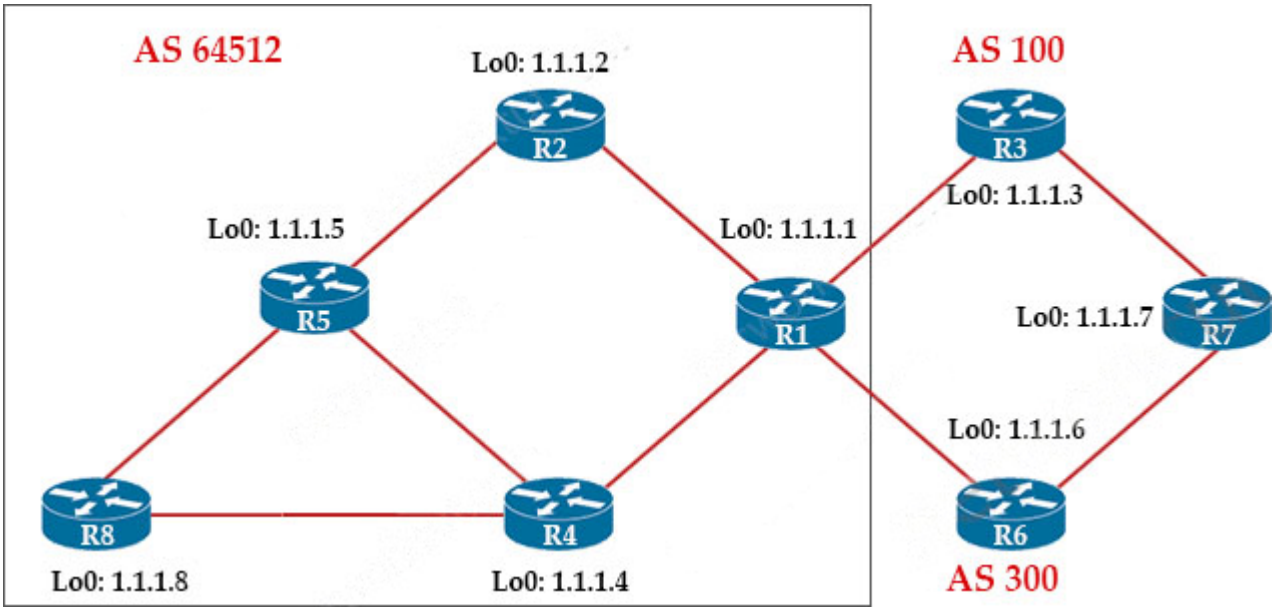
Answer:

label edge router	penultimate hop popping
label switch router	label edge router
forwarding equivalence class	forwarding equivalence class
penultimate hop popping	label switch router

Explanation:
+ allows an LSR to remove the label before forwarding the packet: penultimate hop popping
+ accepts unlabeled packets and imposes labels: label edge router
+ group of packets that are forwarded in the same manner: forwarding equivalence class
+ receives labeled packets and swaps labels: label switch router
A label edge router (LER, also known as edge LSR) is a router that operates at the edge of an MPLS network and acts as the entry and exit points for the network. LERspush an MPLS label onto an incoming packet and pop it off an outgoing packet. A forwarding equivalence class (FEC) is a term

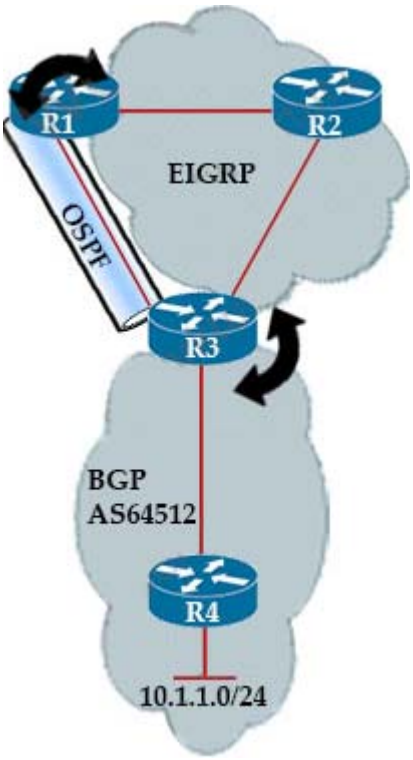
192.Which two protocols work in the control plane of P routers across the MPLS cloud? (choose two)
A. LSP
B. RSVP
C. ECMP
D. LDP
E. MPLS OAM
Answer: B D

193.Exhibit:



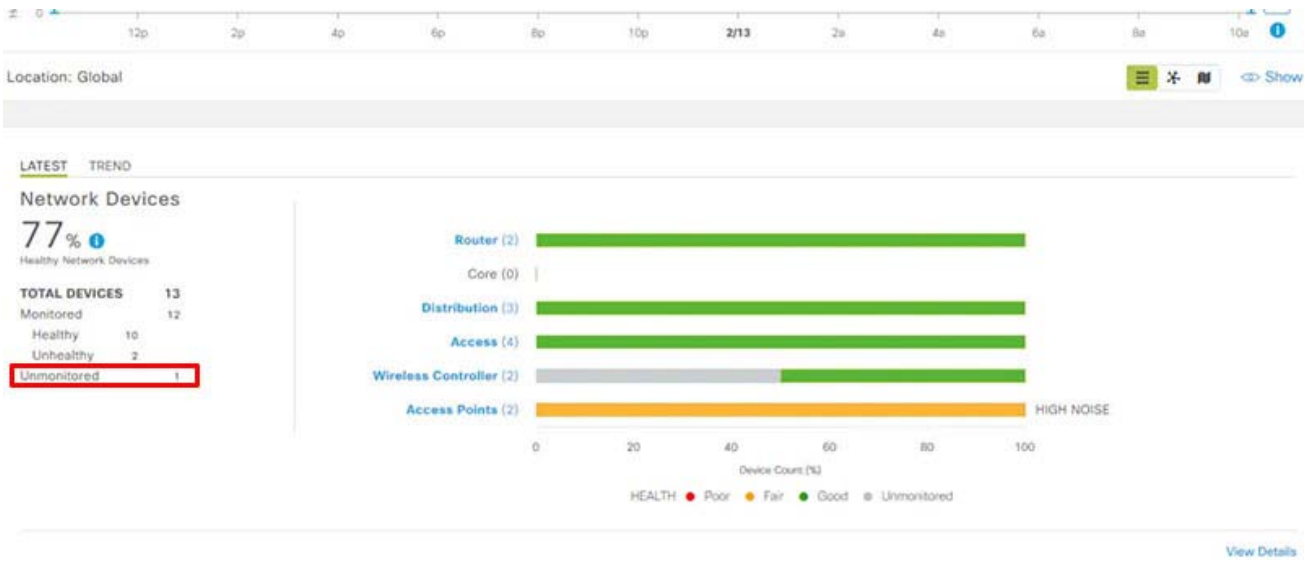
An engineer configured R2 and R5 as route reflectors and noticed that not all routes are sent to R1 to advertise to the eBGP peers.
Which iBGP routers must be configured as route reflectors to advertise all routes to restore reachability across all networks?
A. R1 and R4
B. R1 and R5
C. R4 and R5
D. R2 and R5
Answer: C
Explanation:
When R2 & R5 are route reflectors (RRs), routes from R4 & R8 are advertised to R5 and R5 advertises to R2. But R2 would drop them as R2 is also a RR. Therefore some routes are missing on R1 to advertise to eBGP peers.
Good reference:
https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2015/pdf/TECRST-2310.pdf
Route reflectors (RR) must be fully iBGP meshed so we cannot configure RR on both R1 and R5.
We should choose routers at the center of the topology RRs, in this case R4 & R5.

194.Refer to exhibit.



Routing protocols are mutually redistributed on R3 and R1. Users report intermittent connectivity to services hosted on the 10.1.1.0/24 prefix. Significant routing update changes are noticed on R3 when the show ip route profile command is run.
How must the services be stabilized?
A. The issue with using BGP must be resolved by using another protocol and redistributing it into EIGRP on R3
B. The routing loop must be fixed by reducing the admin distance of iBGP from 200 to 100 on R3
C. The routing loop must be fixed by reducing the admin distance of OSPF from 110 to 80 on R3
D. The issue with using iBGP must be fixed by running eBGP between R3 and R4
Answer: B
Explanation:
After redistribution, R3 learns about network 10.1.1.0/24 via two paths:
+ Internal BGP (IBGP): advertised from R4 with AD of 200 (and metric of 0)
+ OSPF: advertised from R1 with AD of 110 (O E2) (and metric of 20)
Therefore R3 will choose the path with the lower AD via OSPF But this is a looped path which is received from R3 -> R2 -> R1 -> R3. So when the advertised route from R4 is expired, the looped path is also expired soon and R3 will reinstall the main path from R4. This is the cause of intermittent connectivity. In order to solve this issue, we can lower the AD of iBGP to a value which is lower than 110 so that it is preferred over OSPF-advertised route.

195.Refer to Exhibit.



A network administrator added one router in the Cisco DNA Center and checked its discovery and health from the Network Health Dashboard. The network administrator observed that the router is still showing up as unmonitored.

What must be configured on the router to mount it in the Cisco DNA Center?

A. Configure router with NetFlow data

B. Configure router with the telemetry data

C. Configure router with routing to reach Cisco DNA Center

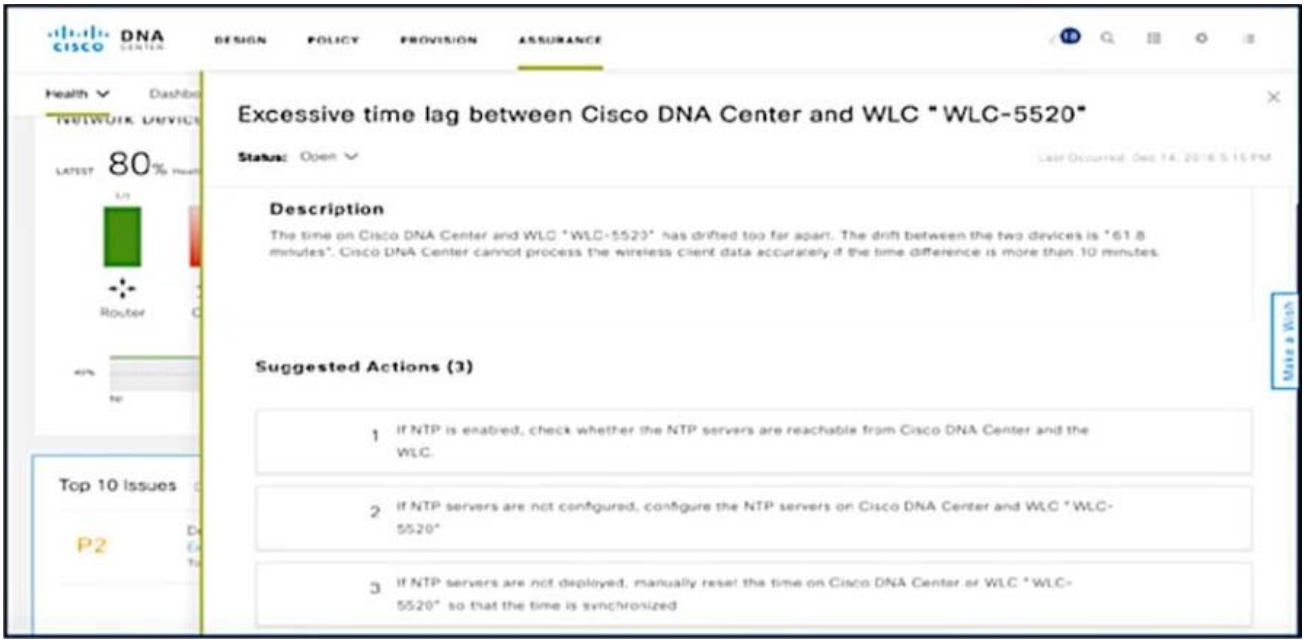
D. Configure router with SNMPv2c or SNMPv3 traps

Answer: B

Explanation:

Unmonitored: Unmonitored devices are devices for which Assurance did not receive any telemetry data during the specified time range.

196.Exhibit:



NTP is configured across the network infrastructure and Cisco DNA Center. An NTP issue was reported on the Cisco DNA Center at 17:15.
Which action resolves the issue?
A. Check and resolve reachability between the WLC and the NTP server
B. Reset the NTP server to resolve any synchronization issues tor all devices
C. Check and resolve reachability between Cisco DNA Center and the NTP server
D. Check and configure NTP on the WLC and synchronize with Cisco DNA Center
Answer: D
Explanation:
Excessive time lag between Cisco DNA Center and device: The time difference between Cisco DNA Center and the device IP Address has drifted too far apart. Cisco DNA Center cannot process the device data accurately if the time difference is more than 3 minutes.
Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/1-2-10/b_cisco_dna_assurance_1_2_10_ug/b_cisco_dna_assurance_1_2_10_ug_chapter_01101.html

197.Refer to Exhibit.

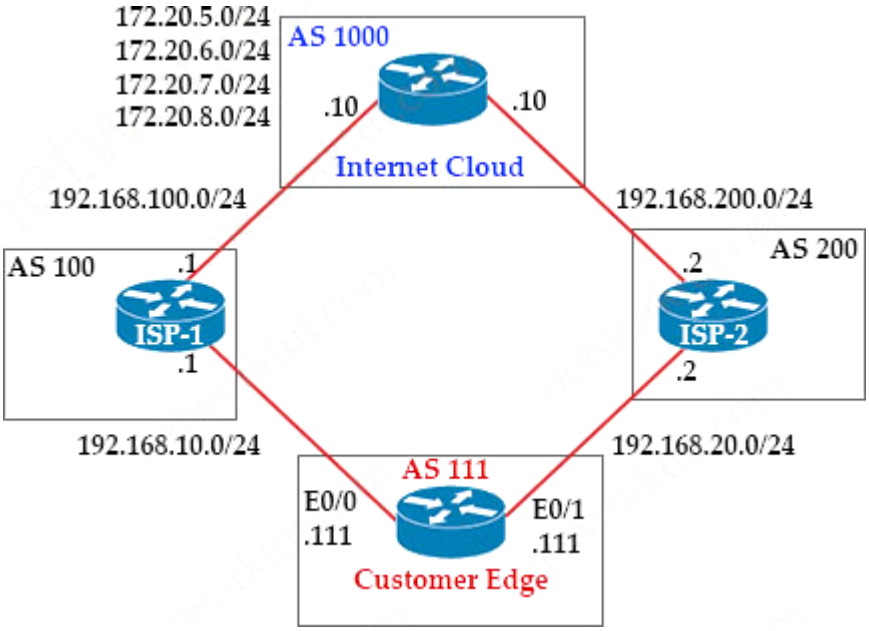
```
Jan 9 15:29:29.713: DHCP_SNOOPING: process new DHCP packet, message type: DHCPINFORM, input interface:
Po2, MAC da: ffff.ffff.ffff, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0
Jan 9 15:29:29.713: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is
flooded to ingress VLAN: (1)
Jan 9 15:29:29.722: DHCP_SNOOPING_SW: bridge packet send packet to cpu port: Vlan1.
Jan 9 15:29:31.509: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Po2 for pak. Was Vl1
Jan 9 15:29:31.509: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Vl1 for pak. Was Po2
Jan 9 15:29:31.509: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Po2 for pak. Was Vl1Jan 9
15:29:31.517: DHCP_SNOOPING: received new DHCP packet from input interface (Port-channel2)
```

A network administrator enables DHCP snooping on the Cisco Catalyst 3750-X switch and configures the uplink port (Port-channel2) as a trusted port. Clients are not receiving an IP address, but when DHCP snooping is disabled, clients start receiving IP addresses.
Which global command resolves the issue?
A. No ip dhcp snooping information option
B. ip dhcp snooping
C. ip dhcp relay information trust portchannel2
D. ip dhcp snooping trust
Answer: A

198.Which configuration feature should be used to block rogue router advertisements instead of using the IPv6 Router Advertisement Guard feature?
A. VACL blocking broadcast frames from nonauthorized hosts
B. PVLANs with promiscuous ports associated to route advertisements and isolated ports for nodes
C. PVLANs with community ports associated to route advertisements and isolated ports for nodes
D. IPv4 ACL blocking route advertisements from nonauthorized hosts
Answer: B
Explanation:
The IPv6 Router Advertisement Guard feature provides support for allowing the network administrator to

block or reject unwanted or rogue router advertisement guard messages that arrive at the network device platform. Router Advertisements are used by devices to announce themselves on the link. The IPv6 Router Advertisement Guard feature analyzes these router advertisements and filters out router advertisements that are sent by unauthorized devices.
Certain switch platforms can already implement some level of rogue RA filtering by the administrator configuring Access Control Lists (ACLs) that block RA ICMP messages that might be inbound on “user” ports.
Reference: https://datatracker.ietf.org/doc/html/rfc6104

199.Refer to Exhibit:

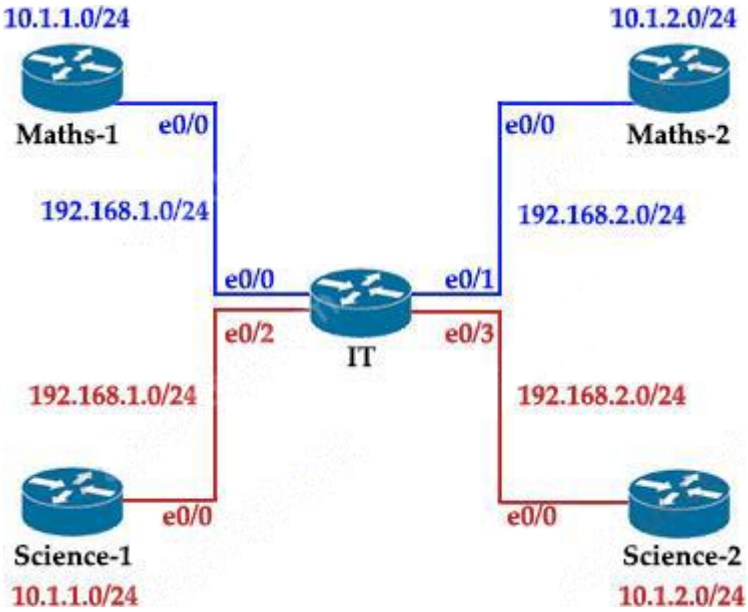



```
ip prefix-list PLIST1 permit 172.20.5.0/24

!
route-map SETLP permit 10
 match ip address prefix-list PLIST1
 set local-preference 90
!
router bgp 111
 neighbor 192.168.10.1 remote-as 100
 neighbor 192.168.10.1 route-map SETLP in
 neighbor 192.168.20.2 remote-as 200
```

AS 111 wanted to use AS 200 as the preferred path for 172.20.5.0/24 and AS 100 as the backup. After the configuration, AS 100 is not used for any other routes.
Which configuration resolves the issue?
A. route-mmap SETLP permit 10
match ip address prefix-list PLIST1
set local-preference 99
route-map SETLP permit 20
B. route-map SETLP permit 10
match ip address prefix-list PLIST1
set local-preference 110

route-map SETLP permit 20
C. router bgp 111
no neighbor 192.168.10.1 route-map SETLP in
neighbor 192.168.10.1 route-map SETLP out
D. router bap 111
no neighbor 192.168.10.1 route-map SETLP in
neighbor 192.168.20.2 route-map SE TLP in
Answer: A
Explanation:
There is an implicit deny all at the end of any route-map so all other traffic that does not match 172.20.5.0/24 would be dropped. Therefore we have to add a permit sequence at the end of the route-map to allow other traffic.
The default value of Local Preference is 100 and higher value is preferred so we have to set the local preference of AS100 lower than that of AS200.

200.Refer to the exhibit.

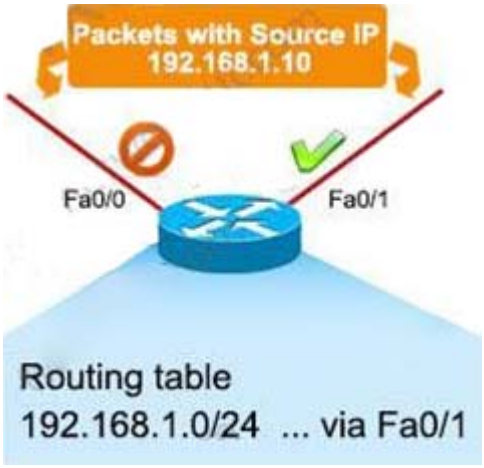


The Math and Science departments connect through the corporate. IT router but users in the Math department must not be able to reach the Science department and vice versa.
Which configuration accomplishes this task?
A. vrf definition Science
interface E 0/2
ip address 192.168.1.1 255.255.255.0
no shut
interface E 0/3
ip address 192.168.2.1 255.255.255.0
no shut
B. vrf definition Science
address-family ipv4
!

interface E 0/2
ip address 192.168.1.1 255.255.255.0
vrf forwarding Science
no shut
!
interface E 0/3
ip address 192.168.2.1 255.255.255.0
vrf forwarding Science
no shut
C. vrf definition Science
address-family ipv4
!
interface E 0/2
ip address 192.168.1.1 255.255.255.0
no shut
!
interface E 0/3
ip address 192.168.2.1 255.255.255.0
no shut
D. vrf definition Science
address-family ipv4
!
interface E 0/2
vrf forwarding Science
ip address 192.168.1.1 255.255.255.0
no shut
!
interface E 0/3
vrf forwarding Science
ip address 192.168.2.1
Answer: D

201.An engineer configured Reverse Path Forwarding on an interface and noticed that the routes are dropped when a route lookup fails on that interface for a prefix that is available in the routing table. Which interface configuration resolves the issue?
A. ip verify unicast source reachable-via rx
B. ip verify unicast source reachable-via any
C. ip verify unicast source reachable-via allow-default
D. ip verify unicast source reachable-via 12-src
Answer: B
Explanation:
According to this question, uRPF is running in strict mode because packets are dropped even when that route exists in the routing table. Maybe packets are dropped because the receiving interface is different from the interface the local router uses to send packets to that destination. The ip verify unicast

source reachable-via rx command enables Unicast RPF in strict mode. To enable loose mode, administrators can use the any option (ip verify unicast source reachable-via any). In loose mode, it doesn't matter if we use this interface to reach the source or not.



The allow-default option allows the use of the default route in the source verification process.

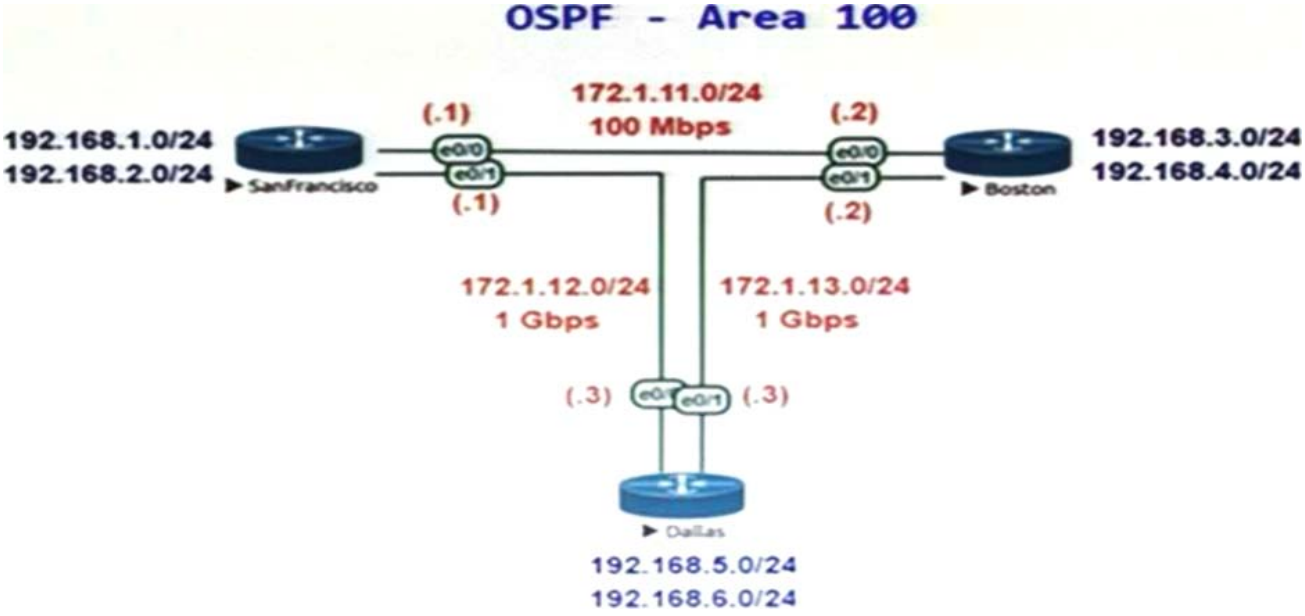
202.Refer to the exhibit.

```
LA
router ospf 1
 network 192.168.12.0 0.0.0.255 area 0
 network 172.16.1.0 0.0.0.255 area 0


NY
router ospf 1
 network 192.168.12.0 0.0.0.255 area 0
 network 172.16.2.0 0.0.0.255 area 0
!
interface E 0/0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 Cisco123
```

The neighbor relationship is not coming up.
Which two configurations bring the adjacency up? (Choose two)
A. NY
router ospf 1
area 0 authentication message-digest
B. LA
interface E 0/0
ip ospf message-digest-key 1 md5 Cisco123
C. NY
interface E 0/0

no ip ospf message-digest-key 1 md5 Cisco123
ip ospf authentication-key Cisco123
D. LA
interface E 0/0
ip ospf authentication-key Cisco123
E. LA
router ospf 1
area 0 authentication message-digest
Answer: BE
Explanation:
The configuration on NY router is good for OSPF authentication. So we must enable
OSPF
authentication on LA router with the following commands:
router ospf 1
area 0 authentication message-digest
interface E0/0
ip ospf message-digest-key 1 md5 Cisco123

203.Refer to the exhibit.



Show IP Route – San Francisco Router

```
Gateway of last resort is not set

     172.1.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.1.11.0/24 is directly connected, Ethernet0/0
L       172.1.11.1/32 is directly connected, Ethernet0/0
C       172.1.12.0/24 is directly connected, Ethernet0/1
L       172.1.12.1/32 is directly connected, Ethernet0/1
O       172.1.13.0/24 [110/11] via 172.1.11.2, 00:02:34, Ethernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Loopback0
L       192.168.1.1/32 is directly connected, Loopback0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, Loopback1
L       192.168.2.1/32 is directly connected, Loopback1
O    192.168.3.0/24 [110/11] via 172.1.11.2, 00:00:44, Ethernet0/0
O    192.168.4.0/24 [110/11] via 172.1.11.2, 00:00:34, Ethernet0/0
O    192.168.5.0/24 [110/11] via 172.1.12.3, 00:00:34, Ethernet0/1
O    192.168.6.0/24 [110/11] via 172.1.12.3, 00:00:24, Ethernet0/1
```

Show IP Route – Boston

```
Gateway of last resort is not set

     172.1.0.0/16 is variably subnetted, 5 subnets, 2 masks
O       172.1.11.0/24 [110/11] via 172.1.13.2, 00:04:44, Ethernet0/1
                      [110/11] via 172.1.12.1, 00:04:44, Ethernet0/0
C       172.1.12.0/24 is directly connected, Ethernet0/0
L       172.1.12.3/32 is directly connected, Ethernet0/0
C       172.1.13.0/24 is directly connected, Ethernet0/1
L       172.1.13.3/32 is directly connected, Ethernet0/1
O    192.168.1.0/24 [110/2] via 172.1.12.1, 00:04:44, Ethernet0/0
O    192.168.2.0/24 [110/2] via 172.1.12.1, 00:04:44, Ethernet0/0
O    192.168.3.0/24 [110/2] via 172.1.13.2, 00:04:44, Ethernet0/1
O    192.168.4.0/24 [110/2] via 172.1.13.2, 00:04:44, Ethernet0/1
     192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.5.0/24 is directly connected, Loopback0
L       192.168.5.1/32 is directly connected, Loopback0
     192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.6.0/24 is directly connected, Loopback1
L       192.168.6.1/32 is directly connected, Loopback1
```

SanFrancisco and Boston routers are choosing slower links to reach each other despite the direct links being up.

Which configuration fixes the issue?

Option A All Routers router ospf 1 auto-cost reference-bandwidth 100	**Option B** Boston Router router ospf 1 auto-cost reference-bandwidth 1000
Option C All Routers router ospf 1 auto-cost reference-bandwidth 1000	**Option D** SanFrancisco Router router ospf 1 auto-cost reference-bandwidth 1000

A. Option A
B. Option B
C. Option C
D. Option D
Answer: C

204.Refer to the exhibit.

Debug output:
username: USER55
password:
Aug 26 12:39:23.813: TPLUS: Queuing AAA Authentication request 4950 for processing
Aug 26 12:39:23.813: TPLUS(00001356) login timer started 1020 sec timeout
Aug 26 12:39:23.813: TPLUS: processing authentication continue request id 4950
Aug 26 12:39:23.813: TPLUS: Authentication continue packet generated for 4950
Aug 26 12:39:23.813: TPLUS(00001356)/0/WRITE/3A72C8D0: Started 5 sec timeout
!
!----- output omitted -----!
!
Aug 26 12:40:01.241: TAC+: using previously set server 192.168.1.3 from group tacacs+
Aug 26 12:40:01.241: TAC+: Opening TCP/IP to 192.168.1.3/49 timeout=5
Aug 26 12:40:01.249: TAC+: Opened TCP/IP handle 0x3BE31D1C to 192.168.1.3/49
Aug 26 12:40:01.249: TAC+: Opened 192.168.1.3 index=1
Aug 26 12:40:01.250: TAC+: 192.168.1.3 (3653537180) AUTHOR/START queued
Aug 26 12:40:01.449: TAC+: (3653537180) AUTHOR/START processed
Aug 26 12:40:01.449: TAC+: (-641430116): received author response status = FAIL
Aug 26 12:40:01.450: TAC+: Closing TCP/IP 0x3BE31D1C connection to 192.168.1.3/49

A network administrator logs into the router using TACACS+ username and password credentials, but the administrator cannot run any privileged commands.
Which action resolves the issue?
A. Configure TACACS+ synchronization with the Active Directory admin group
B. Configure the username from a local database
C. Configure full access for the username from TACACS+ server
D. Configure an authorized IP address for this user to access this router
Answer: C

205.Refer to the exhibit.

```
ipv6 access-list INTERNET
 permit ipv6 2001:DB8:AD59:BA21::/64 2001:DB8:C0AB:BA14::/64
 permit tcp 2001:DB8:AD59:BA21::/64 2001:DB8:C0AB:BA13::/64 eq telnet
 permit tcp 2001:DB8:AD59:BA21::/64 any eq http
 permit ipv6 2001:DB8:AD59::/48 any
 deny ipv6 any any log
```

When monitoring an IPv6 access list, an engineer notices that the ACL does not have any hits and is causing unnecessary traffic to pass through the interface.

Which command must be configured to resolve the issue?

A. access-class INTERNET in

B. ipv6 traffic-filter INTERNET in

C. ipv6 access-class INTERNET in

D. ip access-group INTERNET in

Answer: C

206.Refer to the exhibit.

```
router ospf 1
 redistribute eigrp 1 subnets route-map EIGRP->OSPF
!
router eigrp 1
 network 10.0.106.0 0.0.0.255
!
route-map EIGRP->OSPF permit 10
 match ip address WAN_PREFIXES
route-map EIGRP->OSPF permit 20
 match ip address LOCAL_PREFIXES
route-map EIGRP->OSPF permit 30
 match ip address VPN_PREFIXES
!
ip prefix-list LOCAL_PREFIXES seq 5 permit 172.16.0.0/12 le 24
ip prefix-list VPN_PREFIXES seq 5 permit 192.168.0.0/16 le 24
ip prefix-list WAN_PREFIXES seq 5 permit 10.0.0.0/8 le 24
!
```

The network administrator configured redistribution on an ASBR to reach to all WAN networks but failed.

Which action resolves the issue?

A. The route map must have the keyword prefix-list to evaluate the prefix list entries

B. The OSPF process must have a metric when redistributing prefixes from EIGRP.

C. The route map EIGRP->OSPF must have the 10.0.106.0/24 entry to exist in one of the three prefix lists to pass

D. EIGRP must redistribute the 10.0.106.0/24 route instead of using the network statement

Answer: A

Explanation:

In order to use a prefix-list in a route-map, we must use the keyword “prefix-list” in the “match” statement. .
For example:
match ip address prefix-list WAN_PREFIXES
Without this keyword, the router will try to find an access-list with the same name instead.

207.How does an MPLS Layer 3 VPN function?
A. set of sites use multiprotocol BGP at the customer site for aggregation
B. multiple customer sites interconnect through service provider network to create secure tunnels between customer edge devices
C. set of sites interconnect privately over the Internet for security
D. multiple customer sites interconnect through a service provider network using customer edge to provider edge connectivity
Answer: D
Explanation:
A Multiprotocol Label Switching (MPLS) Layer 3 Virtual Private Network (VPN) consists of a set of sites that are interconnected by means of an MPLS provider core network. At each customer site, one or more customer edge (CE) routers attach to one or more provider edge (PE) routers.
Reference: https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-5/lxvpn/configuration/guide/b-l3vpn-cg-asr9000-65x/b-l3vpn-cg-asr9000-65x_chapter_010.pdf

208.Refer to the exhibit.
Configuration Output

```
aaa new-model
!
aaa authentication login default local
aaa authentication login VTY_AUTH local
aaa authorization exec default none
aaa authorization exec VTY_AUTH local
aaa accounting exec default start-stop group radius
!

password 7 KQAyUutfDrf0g04s
authorization exec VTY_AUTH
login authentication VTY_AUTH

!
```

Debug Output:

```
AAA/AUTHEN/LOGIN (000004B6): Pick method list 'default'
AAA/AUTHOR (0x486): Pick method list 'VTY_AUTH'
AAA/AUTHOR/EXEC(000004B6): Authorization FAILED
```

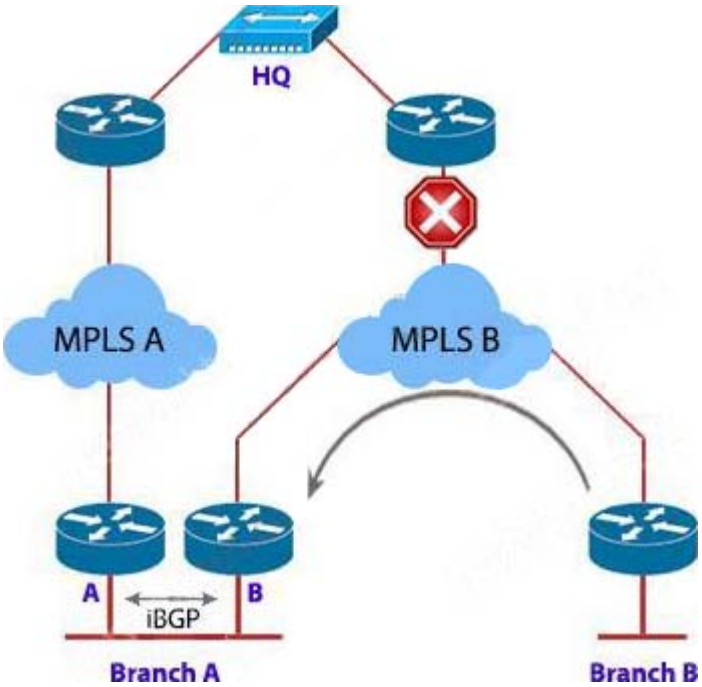
Which action resolves the failed authentication attempt to the router?
A. Configure aaa authorization login command on line vty 0 4
B. Configure aaa authorization login command on line console 0
C. Configure aaa authorization console global command

D. Configure aaa authorization console command on line vty 0 4
Answer: C
Explanation:
In the debug output, we see that the Authorization (not Authentication) failed so we need to correct the authorization. In order to enable authorization, we must use the global command “aaa authorization console” first.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-a1.html

209.A customer reports to the support desk that they cannot print from their PC to the local printer id:401987778.
Which tool must be used to diagnose the issue using Cisco DNA Center Assurance?
A. application trace
B. path trace
C. ACL trace
D. device trace
Answer: B

210.When determining if a system is capable of support, what is the minimum time spacing required for a BFD control packet to receive once a control packet is arrived?
A. Desired Min TX Interval
B. Detect Mult
C. Required Min RX Interval
D. Required Min Echo RX Interval
Answer: C
Explanation:
Desired Min TX Interval: This is the minimum interval, in microseconds, that the local system would like to use when transmitting BFD Control packets, less any jitterapplied. The value zero is reserved.
Required Min Echo RX Interval: This is the minimum interval, in microseconds, between received BFD Echo packets that this system is capable of supporting, less anyjitter applied by the sender. If this value is zero, the transmitting system does not support the receipt of BFD Echo packets.
Reference: https://tools.ietf.org/html/rfc5880

211.Refer to the exhibit.



Troubleshoot and ensure that branch B only ever uses the MPLS B network to reach HQ.
Which action achieves this requirement?
A. Introduce an AS path filter on branch A routers so that only local prefixes are advertised into BGP
B. increase the local preference for all HQ prefixes received at branch B from the MPLS B network to be higher than the local preferences used on the MPLS A network
C. Introduce AS path prepending on the branch A MPLS B network connection so that any HQ advertisements from branch A toward the MPLS B network are prepended three times
D. Modify the weight of all HQ prefixes received at branch B from the MPLS B network to be higher than the weights used on the MPLS A network
Answer: A
Explanation:
If we modify the weight, increase local preference or use AS path prepending then we can only make MPLS B prefer over MPLS A. But when MPLS B is down then MPLS A will be used which does not meet the requirement of this question. Only with AS path filtering we can deny prefixes from certain AS and make sure branch B never uses MPLS A to reach HQ.

212.DRAG DROP
Drag and drop the LDP features from the left onto the descriptions on the right

implicit null label	provides ways of improving load balancing by eliminating the need for DPI at transit LSRs
explicit null label	LSR receives an MPLS header with the label set to 3
inbound label binding filtering	packet is encapsulated in MPLS with the option of copying the IP precedence to EXP bits
entropy label	controls the amount of memory used to store LDP label bindings advertised by other devices

Answer:

implicit null label	entropy label
explicit null label	implicit null label
inbound label binding filtering	explicit null label
entropy label	inbound label binding filtering

Explanation:

The MPLS LDP Inbound Label Binding Filtering feature can be used to control the amount of memory used to store Label Distribution Protocol (LDP) label bindings advertised by other devices. For example, in a simple Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment, the VPN provider edge (PE) devices might require label switched paths (LSPs) only to their peer PE devices (that is, they do not need LSPs to core devices). Inbound label binding filtering enables a PE device to accept labels only from other PE devices.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/15-sy/mp-ldp-15-sy-boo
k/mp-ldp-inbound-filtr.html

213.Refer to the exhibit.

```
Router# show ip route

   2.0.0.0/24 is subnetted, 1 subnets
C     2.2.2.0 is directly connected, Ethernet0/0
C  3.0.0.0/8 is directly connected, Serial1/0
O E2 200.1.1.0/24 [110/20] via 2.2.2.2, 00:16:17, Ethernet0/0
O E1 200.2.2.0/24 [110/104] via 2.2.2.2, 00:00:41, Ethernet0/0
   131.108.0.0/24 is subnetted, 2 subnets
O     131.108.2.0 [110/74] via 2.2.2.2, 00:16:17, Ethernet0/0
O IA   131.108.1.0 [110/84] via 2.2.2.2, 00:16:17, Ethernet0/0

Router# show ip bgp

Network          Next Hop     Metric LocPrf Weight Path
*> 2.2.2.0/24     0.0.0.0          0    32768 ?
*> 131.108.1.0/24 2.2.2 2          84      32768 ?
*> 131.108.2.0/24 2.2.2.2          74      32768 ?
```

The OSPF routing protocol is redistributed into the BGP routing protocol, but not all the OSPF routes are distributed into BGP.

Which action resolves the issue?

A. Include the word external in the redistribute command

B. Use a route-map command to redistribute OSPF external routes defined in an access list

C. Include the word internal external in the redistribute command

D. Use a route-map command to redistribute OSPF external routes defined in a prefix list.

Answer: C

Explanation:

If you configure the redistribution of OSPF into BGP without keywords, only OSPF intra-area and inter-area routes are redistributed into BGP, by default. You can use the internal keyword along with the redistribute command under router bgp to redistribute OSPF intra- and inter-area routes.

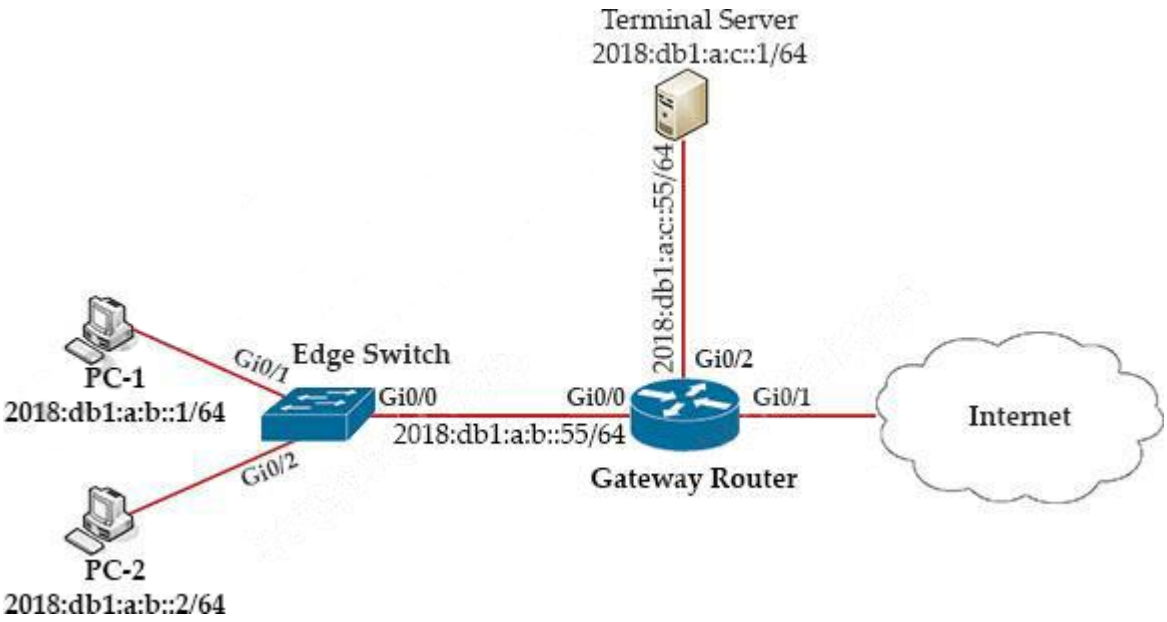
Use the external keyword along with the redistribute command under router bgp to redistribute OSPF external routes into BGP.

-> In order to redistribute all OSPF routes into BGP, we must use both internal and external keywords. The full command would be (suppose we are using OSPF 1): redistribute ospf 1 match internal external

Note: The configuration shows match internal external 1 external 2. This is normal because OSPF automatically appends “external 1 external 2” in the configuration. In other words, keyword external = external 1 external 2. External 1 = O E1 and External 2 = O E2.

Reference: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/5242-bgp-ospf-redis.html

214.Refer to the exhibit.



Gateway-Router# show ipv6 access-list
IPv6 access list Default_Access
permit tcp host 2018:DB1: A: B::1 host 2018:DB1:A:C::1 eq www sequence 10
deny tcp any host 2018:DB1: A:C::1 eq telnet sequence 20
permit tcp host 2018:DB1: A: B::2 host 2018:DB1:A:C::1 eq telnet sequence 30
permit ipv6 2018:DB1: A: B::/64 any sequence 40
PC-2 failed to establish a Telnet connection to the terminal server.
Which configuration resolves the issue?
A. Gateway-Router(config)#ipv6 access-list Default Access
Gateway-Router(config-ipv6-acl)#sequence 15 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C. :1 eq telnet
B. Gateway-Router(config)#ipv6 access-list Default Access
Gateway-Router(config-ipv6-acl)#permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet
C. Gateway-Router(config)#ipv6 access-list Default Access
Gateway-Router(config-ipv6-acl)#no sequence 20
Gateway-Router(config-ipv6-acl)#sequence 5 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet
D. Gateway-Router(config)#fipv6 access-list Default Access
Gateway-Router(confia-ipv6-acl)#sequence 25 permit tcp host 2018:DB1:A:B:2 host 2018:DB1:A:C. :1 eq telnet
Answer: A
Explanation:
In fact in this question both answer A and answer C are correct but we believe answer A is the better choice as it only allows PC-2 to telnet to terminal server. All other hosts are refused to telnet to terminal server via sequence 20.

215.What statement about route distinguishes in an MPLS network is true?
A. Route distinguishes make a unique VPNv4 address across the MPLS network.
B. Route distinguishers allow multiple instances of a routing table to coexist within the edge router.

C. Route distinguishes are used for label bindings
D. Route distinguishes define which prefixes are imported and exported on the edge router
Answer: A

216.Refer to the exhibit.

```
Router#show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(1)
                    Xmit Queue   PeerQ        Mean   Pacing Time   Multicast    Pending
Interface           Peers Un/Reliable Un/Reliable SRTT  Un/Reliable Flow Timer  Routes
Lo0                   0     0/0       0/0         0     0/0          0           0
Fa0/0                 1     0/0       0/0         7     0/2          50          0

Router#show running-config | section eigrp
router eigrp 1
 network 172.16.0.0 0.0.0.255
 network 192.168.2.2 0.0.0.0
 network 192.168.12.2 0.0.0.0

Router#show running-config interface Fa0/3
Building configuration...


Current configuration : 93 bytes
!
interface FastEthernet0/3
 ip vrf forwarding CLIENT1
 ip address 172.16.0.1 255.255.255.0
```

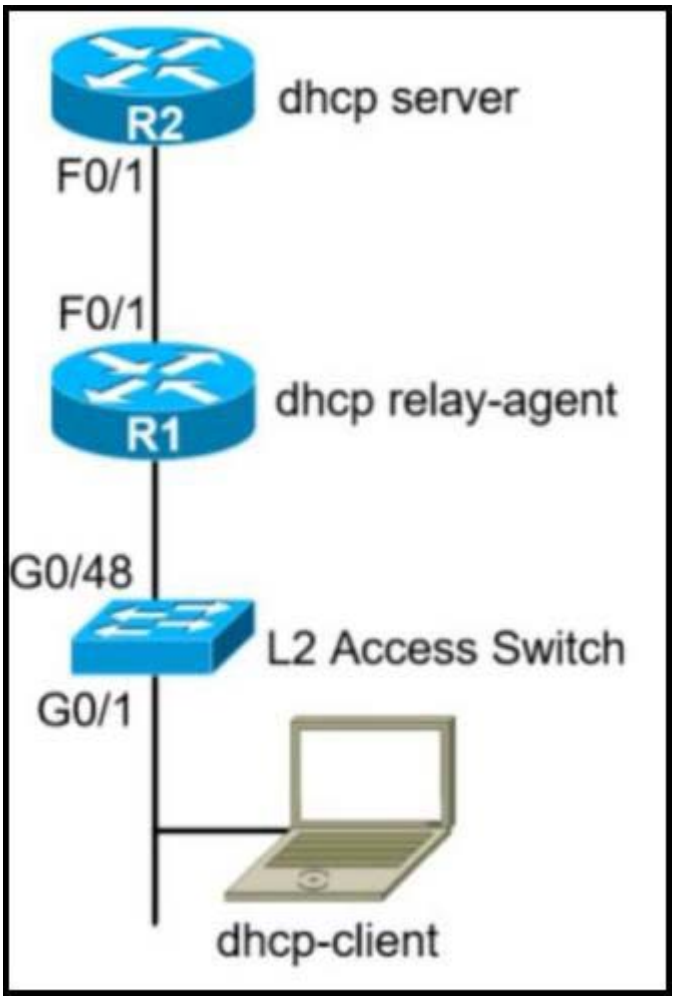
While troubleshooting an EIGRP neighbor adjacency problem, the network engineer notices that the interface connected to the neighboring router is not participating in the EIGRP process.
Which action resolves the issues?
A. Configure the network command to network 172.16.0.1 0.0.0.0
B. Configure the network command under EIGRP address family vrf CLIENT1
C. Configure EIGRP metrics on interface FastEthernet0/3
D. Configure the network command under EIGRP address family ipv4
Answer: B

217.Refer to the exhibit.

```
admin@linux:~$ scp script.py admin@198.51.100.64:script.py
Password:
Administratively disabled.
admin@linux:~$ Connection to 198.51.100.64 closed by remote
host.
```

A network administrator has developed a Python script on the local Linux machine and is trying to transfer it to the router. However, the transfer fails.
Which action resolves this issue?
A. The SSH service must be enabled with the crypto key generate rsa command.
B. The SCP service must be enabled with the ip scp server enable command.
C. The Python interpreter must first be enabled with the guestshell enable command.
D. The SSH access must be allowed on the VTY lines using the transport input ssh command.
Answer: B

218.Refer to the exhibit.



The network administrator can see the DHCP discovery packet in R1. but R2 is not replying to the DHCP request. The R1 related interface is configured with the DHCP helper address. If the PC is directly connected to the FaO/1 interface on R2, the DHCP server assigns as IP address from the DHCP pool to the PC.

Which two commands resolve this issue? (Choose two.)

A. service dhcp-relay command on R1

B. ip dhcp option 82 command on R2

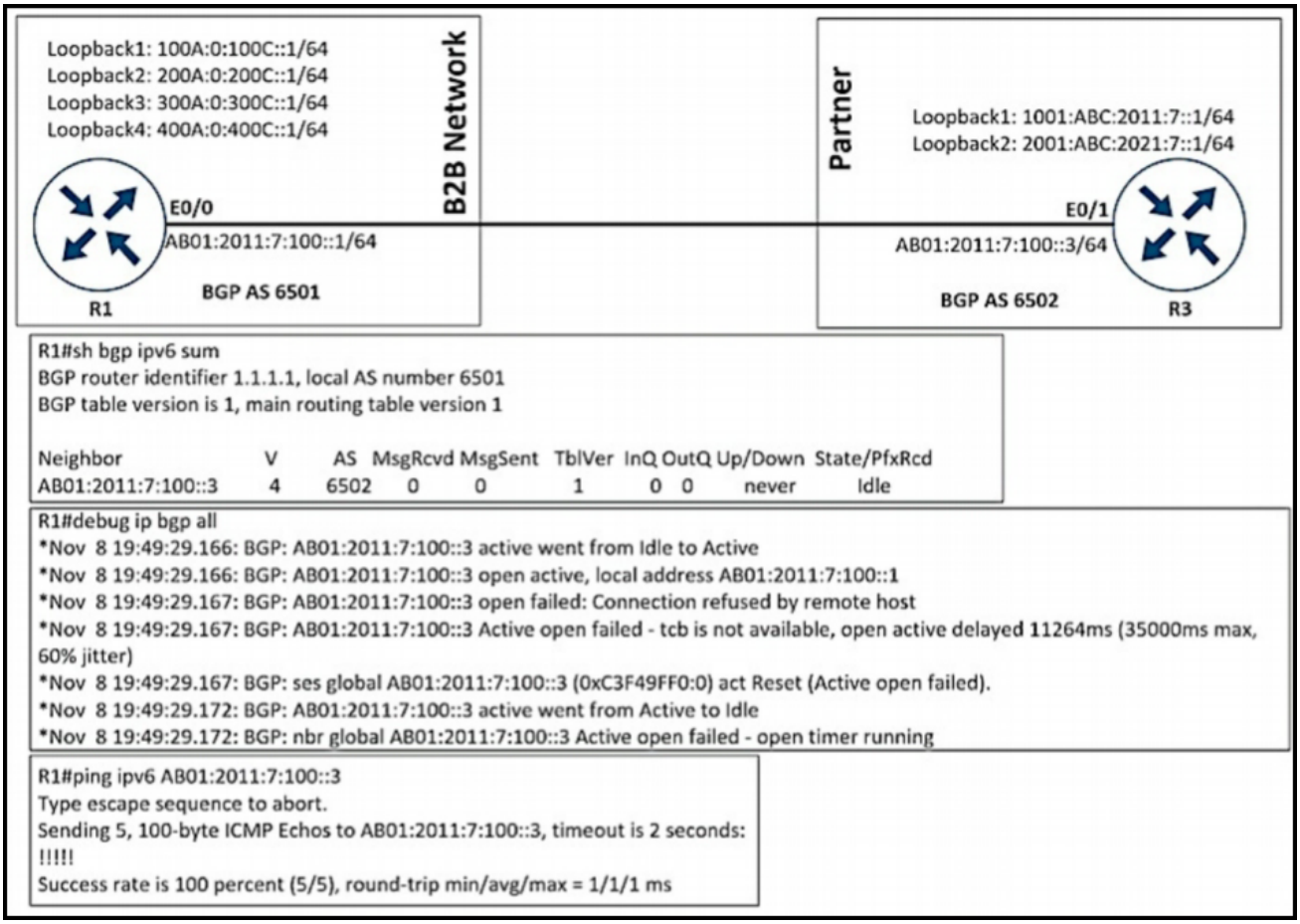
C. service dhcp command on R1

D. ip dhcp relay information enable command on R1

E. ip dhcp relay information trust-all command on R2

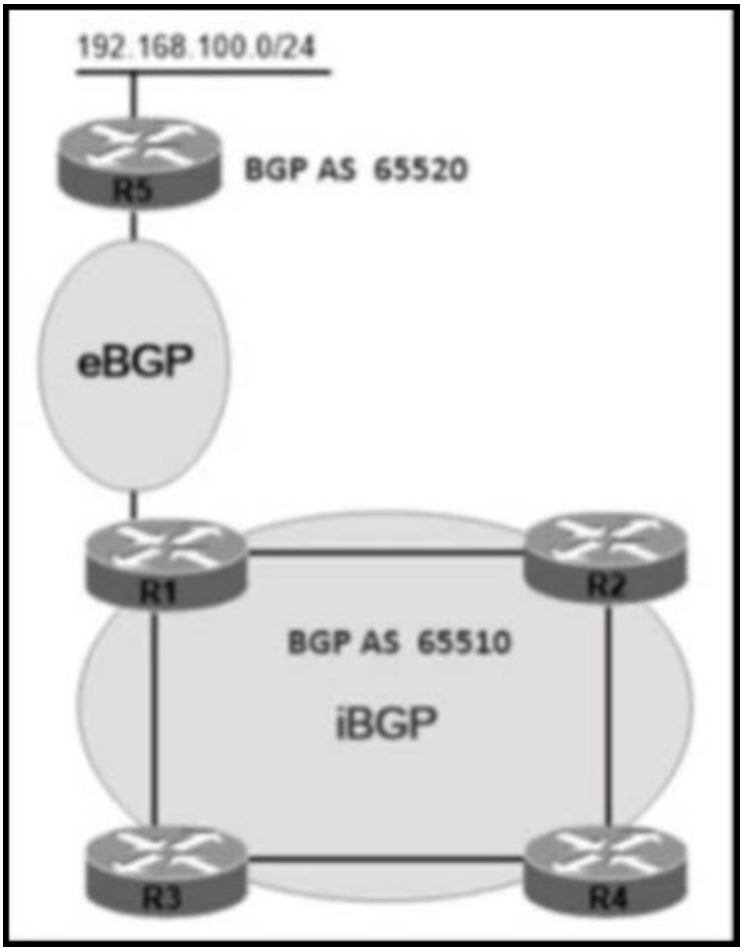
Answer: BC

219.Refer to the exhibit.



An engineer configured BGP between routers R1 and R3 The BOP peers cannot establish neighbor adjacency to be able to exchange routes.
Which configuration resofves this issue?
A. R3
router bgp 6502
address-family ipv6
neighbor AB01:2011:7:100::1 activate
B. R1
router bgp 6501
address-family ipv6
neighbor AB01:2011:7:100;:3 activate
C. R3
router bgp 6502
neighbor AB01:2011:7:100::1 ebgp-muttlhop 255
D. R1
router bgp 6501 neighborAB01:2011:7:100::3ebgp-multihop255
Answer: A

220.Refer to the exhibit.



AS65510 iBGP is configured for directly connected neighbors. R4 cannot ping or traceroute network 192 168.100.0/24.

Which action resolves this issue?

A. Configure R4 as a route reflector server and configure R1 as a route reflector client

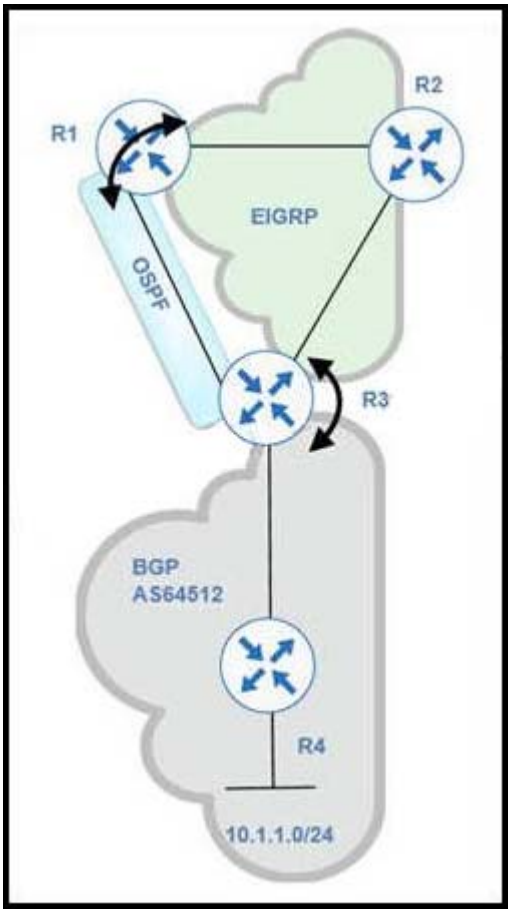
B. Configure R1 as a route reflector server and configure R2 and R3 as route reflector clients

C. Configure R4 as a route reflector server and configure R2 and R3 as route reflector clients.

D. Configure R1 as a route reflector server and configure R4 as a route reflector client

Answer: C

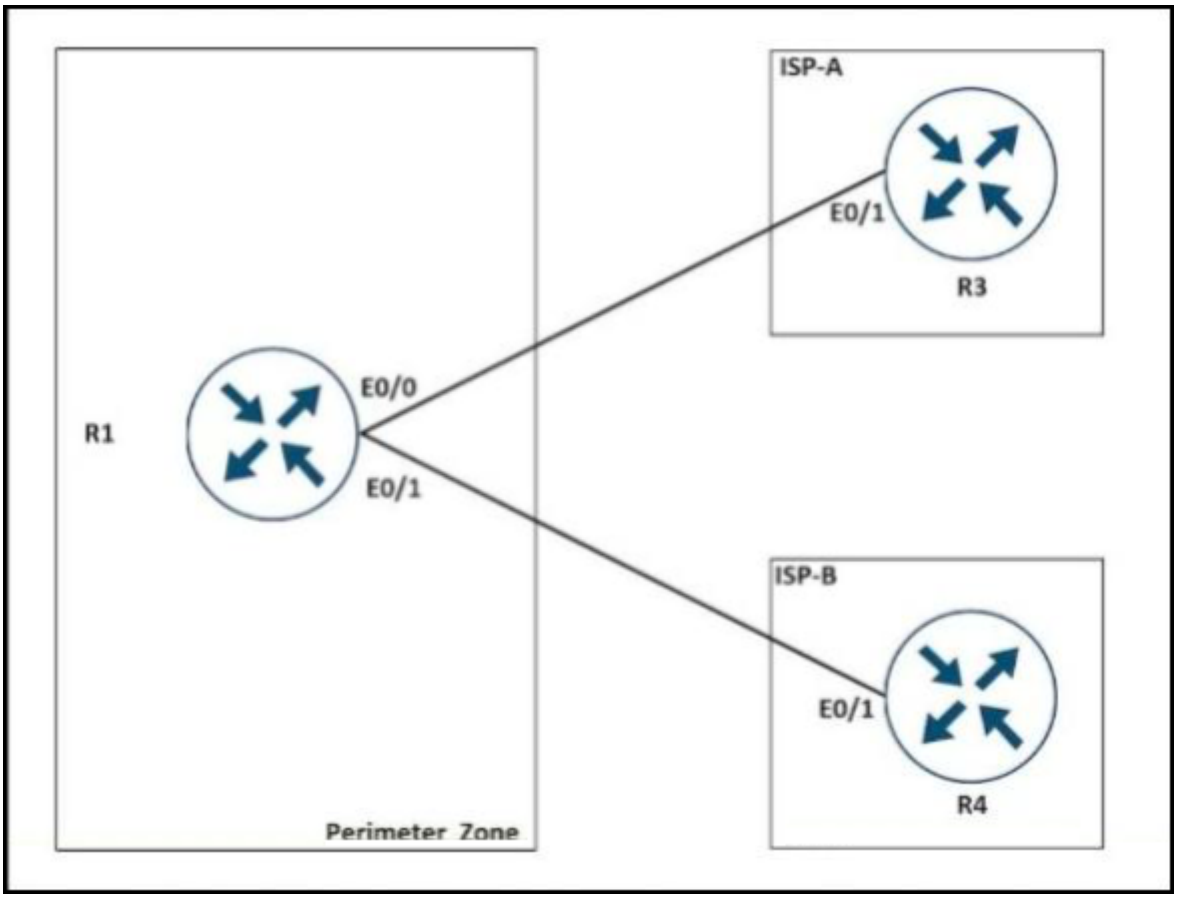
221.Refer to the exhibit.



BGP and EIGRP are mutually redistributed on R3, and EIGRP and OSPF are mutually redistributed on R1. Users report packet loss and interruption of service to applications hosted on the 10.1.1.0724 prefix. An engineer tested the link from R3 to R4 with no packet loss present but has noticed frequent routing changes on R3 when running the debug ip route command.
Which action stabilizes the service?
A. Tag the 10.1.1.0/24 prefix and deny the prefix from being redistributed into OSPF on R1.
B. Repeat the test from R4 using ICMP ping on the local 10.1.1.0/24 prefix, and fix any Layer 2 errors on the host or switch side of the subnet. ^
C. Place an OSPF distribute-list outbound on R3 to block the 10.1.10/24 prefix from being advertised back to R3.
D. Reduce frequent OSPF SPF calculations on R3 that cause a high CPU and packet loss on traffic traversing R3.
Answer: A
Explanation:
After redistribution, R3 learns about network 10.1.1.0/24 via two paths:
+ Internal BGP (IBGP): advertised from R4 with AD of 200 (and metric of 0)
+ OSPF: advertised from R1 with AD of 110 (O E2) (and metric of 20) Therefore R3 will choose the path with the lower AD via OSPF
But this is a looped path which is received from R3 -> R2 -> R1 -> R3. So when the advertised route from R4 is expired, the looped path is also expired soon and R3 will reinstall the main path from R4. This is the cause of intermittent connectivity.
We can solve this problem by denying the 10.1.1.0/24 prefix from being redistributed into OSPF on R1.

So R3 will not learn this prefix from R1.
Or another solution is to place an OSPF distribute-list inbound on R3 to block the 10.1.1.0/24 prefix from being advertised back to R3.

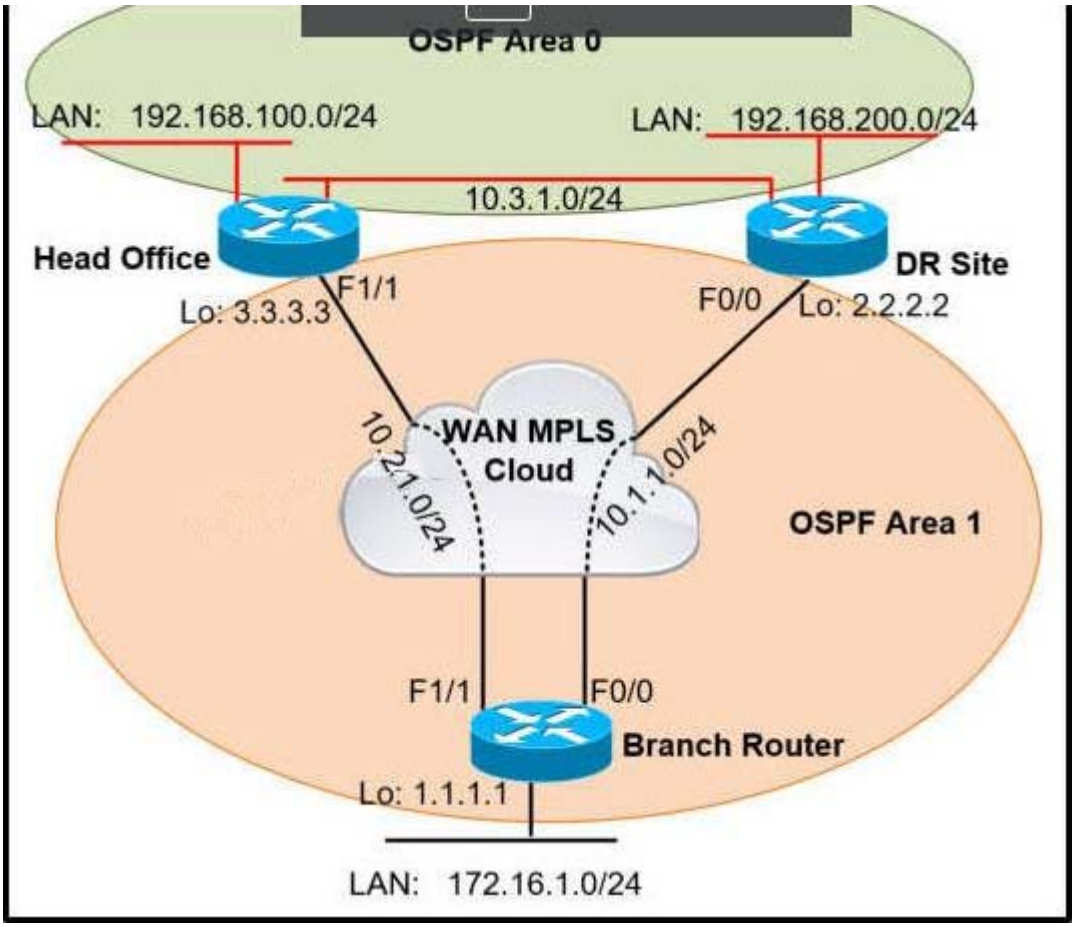
222.Refer to the exhibit.



A network is under a cyberattack. A network engineer connected to R1 by SSH and enabled the terminal monitor via SSH session to find the source and destination of the attack. The session was flooded with messages, which made it impossible for the engineer to troubleshoot the issue.
Which command resolves this issue on R1?
A. no terminal monitor
B. (config)#terminal no monitor
C. #terminal no monitor
D. (config)#no terminal monitor
Answer: C

223.Refer to the exhibit.

```
Branch-Router#
*Nov 29 15:20:22.415: OSPF-1 HELLO Fa1/1: Rcv hello from 3.3.3.3 area 1 10.2.1.3
*Nov 29 15:20:23.195: OSPF-1 HELLO Fa1/1: Send hello to 224.0.0.5 area 1 from 10.2.1.1

Branch-Router#
*Nov 29 15:20:27.955: OSPF-1 HELLO Fa0/0: Rcv hello from 2.2.2.2 area 1 10.1.1.2
*Nov 29 15:20:27.955: OSPF-1 HELLO Fa0/0: Mismatched hello parameters from 10.1.1.2
*Nov 29 15:20:27.955: OSPF-1 HELLO Fa0/0: Dead R 40 C 40, Hello R 10 C 10 Mask R 255.255.255.0 C 255.255.255.240
*Nov 29 15:20:28.311: OSPF-1 HELLO Fa0/0: Send hello to 224.0.0.5 area 1 from 10.1.1.1
```



A network administrator reviews the branch router console log to troubleshoot the OSPF adjacency issue with the DR router.

Which action resolves this issue?

A. Advertise the branch WAN interface matching subnet for the DR site.

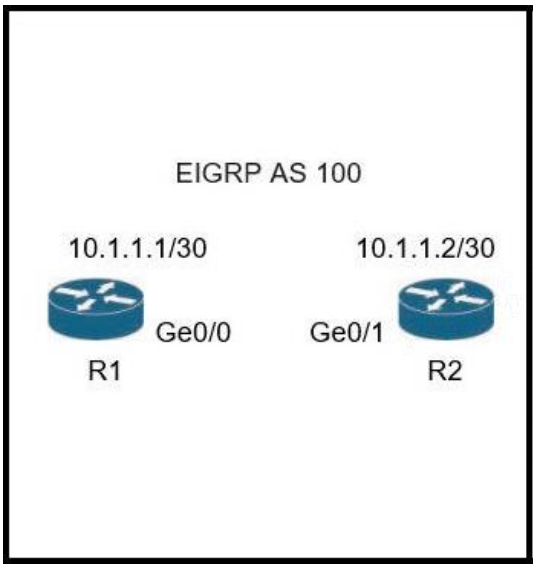
B. Configure matching hello and dead intervals between sites.

C. Configure the WAN interface for DR site in the related OSPF area.

D. Stabilize the DR site flapping link to establish OSPF adjacency.

Answer: B

224.Refer to the exhibit.




```
R1# debug eigrp packets
(UPDATE, REQUEST, QUERY, REPLY, HELLO,
UNKNOWN, PROBE, ACK, STUB, SIAQUERY,
SIAREPLY)
EIGRP Packet debugging is on
R1#
EIGRP: Sending HELLO on Gi0/0 - paklen 20
AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0
iidbQ un/rely 0/0
R1#
EIGRP: Sending HELLO on Gi0/0 - paklen 20
AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0
iidbQ un/rely 0/0
```

Which action resolves the adjacency issue?

A. Match the hello interval timers.

B. Configure the same EIGRP process IDs.

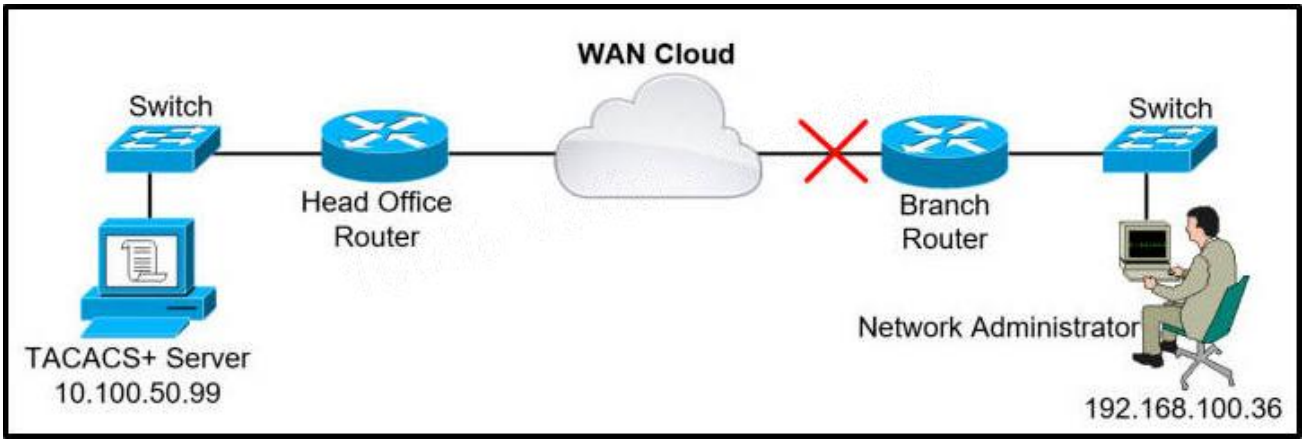
C. Match the authentication keys.

D. Configure the same autonomous system numbers.

Answer: D

225. Topic 3, Exam Pool C

Refer to the exhibit.



A network administrator is trying to access a branch router using TACACS+ username and password credentials, but the administrator cannot log in to the router because the WAN connectivity is down. The branch router has following AAA configuration:

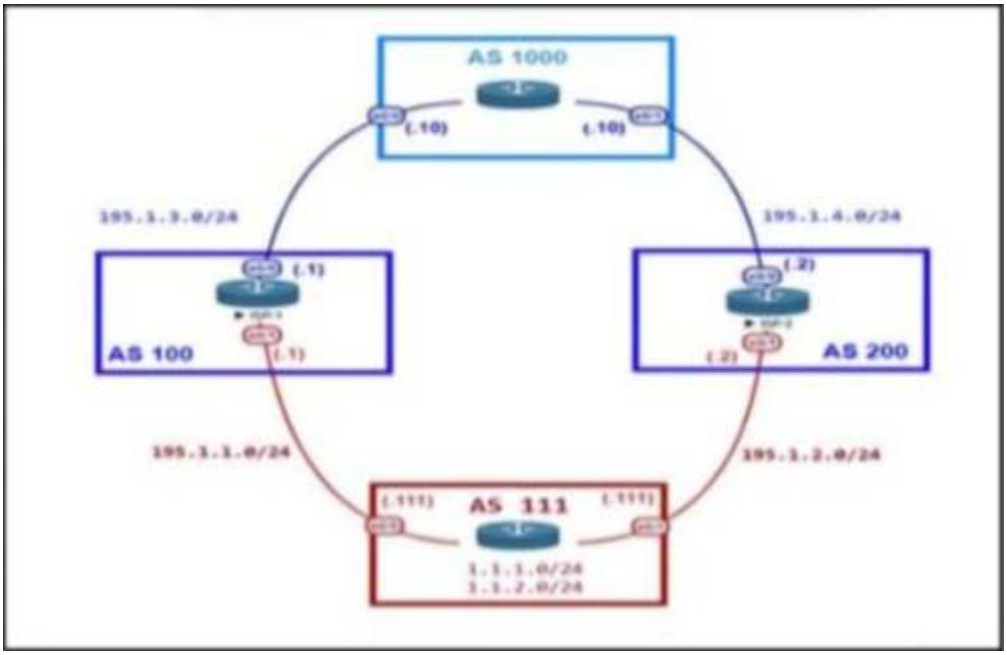
```
aaa new-model
aaa authorization commands 15 default group tacacs+
aaa accounting commands 1 default stop-only group tacacs+
aaa accounting commands 15 default stop-only group tacacs+
tacacs-server host 10.100.50.99
tacacs-server key CI$co123
```

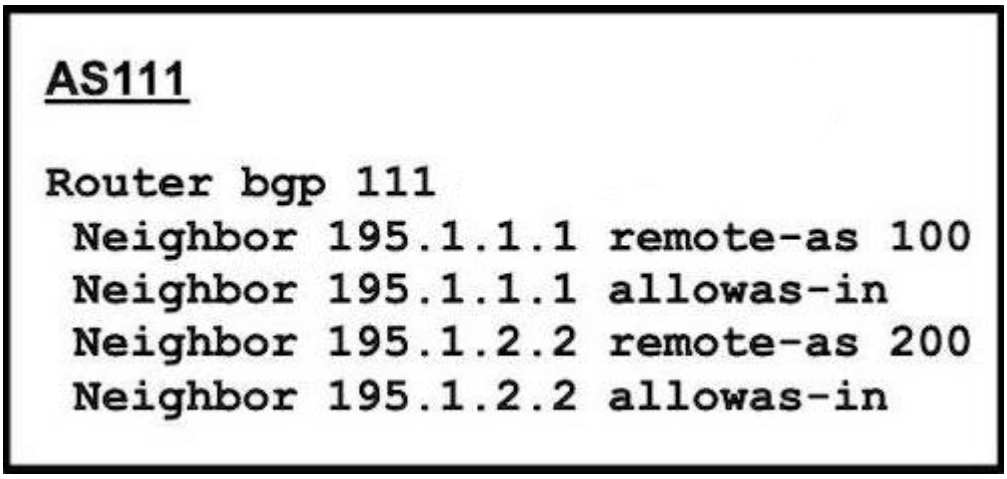
Which command will resolve this problem when WAN connectivity is down?
A. aaa authentication login default group tacacs+ local
B. aaa authentication login default group tacacs+ enable
C. aaa authentication login default group tacacs+ console
D. aaa authentication login console group tacacs+ enable
Answer: A

226.Users report issues with reachability between areas as soon as an engineer configured summary routes between areas in a multiple area OSPF autonomous system.
Which action resolves the issue?
A. Configure the summary-address command on the ASBR.
B. Configure the summary-address command on the ABR.
C. Configure the area range command on the ABR.
D. Configure the area range command on the ASBR.
Answer: D

227.A network administrator is troubleshooting a high utilization issue on the route processor of a router that was reported by NMS. The administrator logged into the router to check the control plane policing and observed that the BGP process is dropping a high number of routing packets and causing thousands of routes to recalculate frequently.
Which solution resolves this issue?
A. Police the cir for BGP, conform-action transmit, and exceed action transmit.
B. Shape the pir for BGP, conform-action set-prec-transmit, and exceed action set-frde-transmit.
C. Shape the cir for BGP. conform-action transmit, and exceed action transmit.
D. Police the pir for BGP, conform-action set-prec-transmit, and exceed action set-clp-transmit.
Answer: A

228.Refer to the exhibit.





AS111 is receiving its own routes from AS200 causing a loop in the network.
Which configuration provides loop prevention?

A)

```
router bgp 111
 neighbor 195.1.1.1 as-override
 neighbor 195.1.2.2 as-override
```

B)

```
router bgp 111
 neighbor 195.1.1.1 as-override
 no neighbor 195.1.2.2 allowas-in
```

C)

```
router bgp 111
 no neighbor 195.1.1.1 allowas-in
 no neighbor 195.1.2.2 allowas-in
```

D)

```
router bgp 111
 neighbor 195.1.2.2 as-override
 no neighbor 195.1.1.1 allowas-in
```

A. Option A
B. Option B
C. Option C
D. Option D
Answer: C

229.Refer to the exhibit.

```
ip address 4.4.4.4 255.255.255.0
!
interface FastEthernet1/0
Description **** WAN link ****
ip address 10.0.0.1 255.255.2555.0
!
interface FastEthernet1/1
Description **** LAN Network ****
ip address 192.168.1.1 255.255.2555.0
!
!
router ospf 1
router-id 4.4.4.4
log-adjacency-changes
network 4.4.4.4 0.0.0.0 area 0
network 10.0.0.1 0.0.0.0 area 0
network 192.168.1.1 0.0.0.0 area 10
!
```

A)

```
interface loopback0
  ip address 4.4.4.4 255.255.255.0
  ip ospf network broadcast
```

B)

```
interface loopback0
  ip address 4.4.4.4 255.255.255.0
  ip ospf interface type network
```

C)

```
interface loopback0
  ip address 4.4.4.4 255.255.255.0
  ip ospf network point-to-point
```

D)

```
interface loopback0
  ip address 4.4.4.4 255.255.255.0
  ip ospf interface area 10
```

A. Option

B. Option

C. Option

D. Option

Answer: A

230.Refer to the exhibit.

```
P 172.29.0.0/16, 1 successors, FD is 307200, serno 2
        via 192.168.254.2 (307200/281600), FastEthernet0/1
        via 192.168.253.2 (410200/352300), FastEthernet0/0
```

When the FastEthemet0/1 goes down, the route to 172.29.0 0/16 via 192.168.253 2 is not installed in the RIB.

Which action resolves the issue?

A. Configure reported distance greater than the feasible distance

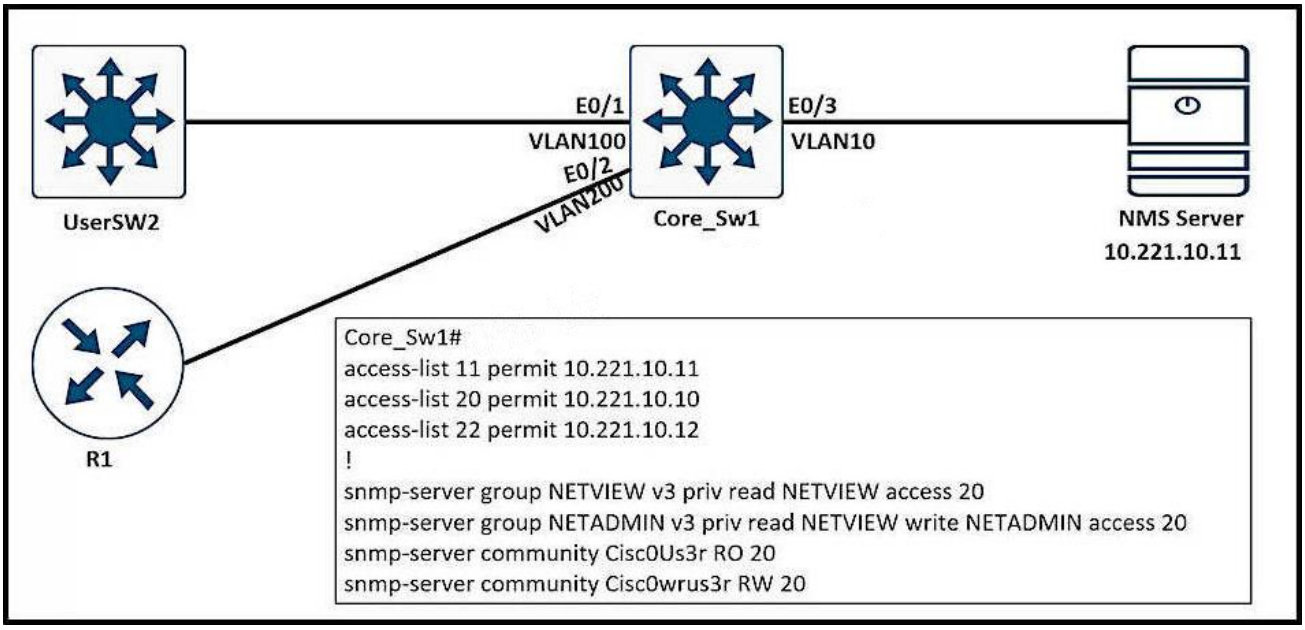
B. Configure feasible distance greater than the successor's feasible distance.

C. Configure reported distance greater than the successor's feasible distance.

D. Configure feasible distance greater than the reported distance

Answer: D

231.Refer to the exhibit.



An engineer configured SNMP communities on the Core_Sw1, but the SNMP server cannot obtain information from Core_Sw1.

Which configuration resolves this issue?

A. access-list 20 permit 10.221.10.12

B. snmp-server group NETVIEW v2c priv read NETVIEW access 20

C. snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22

D. access-list 20 permit 10.221.10.11

Answer: D

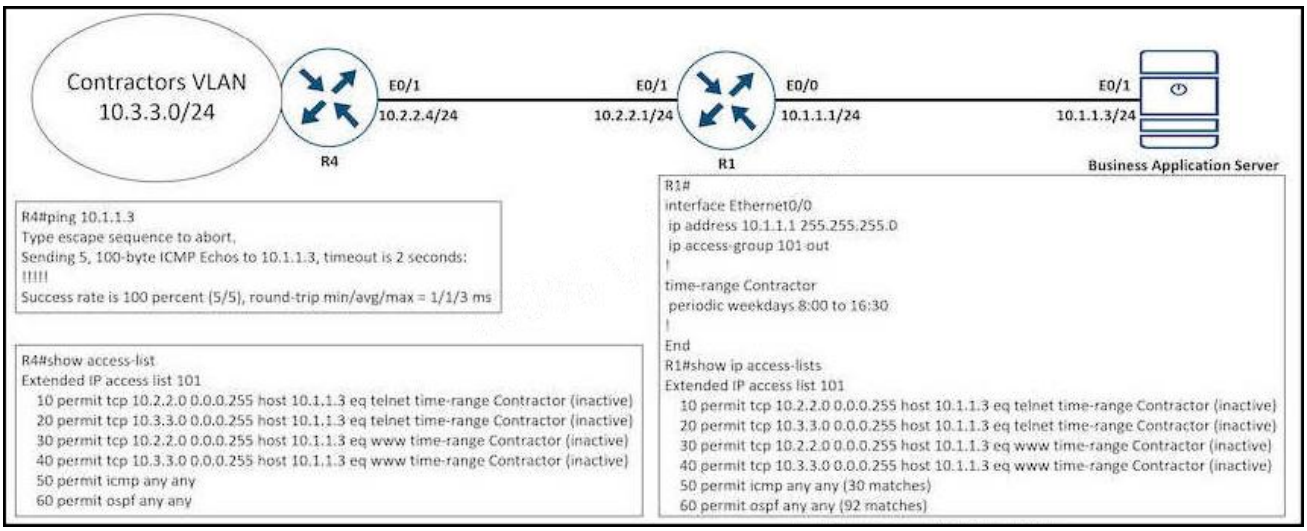
232.IPv6 is enabled in the infrastructure to support customers with an IPv6 network over WAN and to connect the head office to branch offices in the local network. One of the customers is already running IPv6 and wants to enable IPv6 over the DMVPN network infrastructure between the headend and branch sites.

Which configuration command must be applied to establish an mGRE IPv6 tunnel neighborship?

A. tunnel protection mode ipv6

B. ipv6 unicast-routing
C. ipv6 nhrp holdtime 30
D. tunnel mode gre multipoint ipv6
Answer: D

233.Refer to the exhibit.



An engineer is troubleshooting failed access by contractors to the business application server via Telnet or HTTP during the weekend.
Which configuration resolves the issue?
A)

R1
time-range Contractor
no periodic weekdays 8:00 to 16:30
periodic daily 8:00 to 16:30

B)
R4
time-range Contractor
no periodic weekdays 17:00 to 23:59
periodic daily 8:00 to 16:30
C)
R4
no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor
D)
R1
no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor
A. Option
B. Option
C. Option
D. Option
Answer: B

234.Refer to the exhibit.

```
Route-map PBR, permit, sequence 10
  Match clauses:
    ip address (access-lists): FILTER_ACL
  Set clauses:
    ip next-hop verify-availability 209.165.202.129 1 track 100  [down]
    ip next-hop verify-availability 209.165.202.131 2 track 200  [up]
  Policy routing matches: 0 packets, 0 bytes
route-map PBR, deny, sequence 20
  Match clauses:
  Set clauses:
    ip next-hop 209.165.201.30
  Policy routing matches: 275364861 packets, 12200235037 bytes
```

An engineer has configured policy-based routing and applied the configured to the correct interface.
How is the configuration applied to the traffic that matches the access list?
A. It is sent to 209.165.202.131.
B. It is sent to 209.165.202.129.
C. It is dropped.
D. It is forwarded using the routing table lookup.
Answer: A

235.How is VPN routing information distributed in an MPLS network?
A. The top level of the customer data packet directs it to the correct CE device
B. It is established using VPN IPsec peers.
C. It is controlled using of VPN target communities.
D. It is controlled through the use of RD.
Answer: C

236.Which mechanism must be chosen to optimize the reconvergence time for OSPF at company location 407173257 that is less CPU-intensive than reducing the hello and dead timers?
A. BFD
B. Dead Peer Detection keepalives
C. SSO
D. OSPF demand circuit
Answer: A

237.A network administrator performed a Compact Flash Memory upgrade on a Cisco Catalyst 6509 Switch. Everything is functioning normally except SNMP, which was configured to monitor the bandwidth of key interfaces but the interface indexes are changed.
Which global configuration resolves the issue?
A. snmp-server ifindex permanent
B. snmp ifindex permanent
C. snmp-server ifindex persist
D. snmp ifindex persist
Answer: D

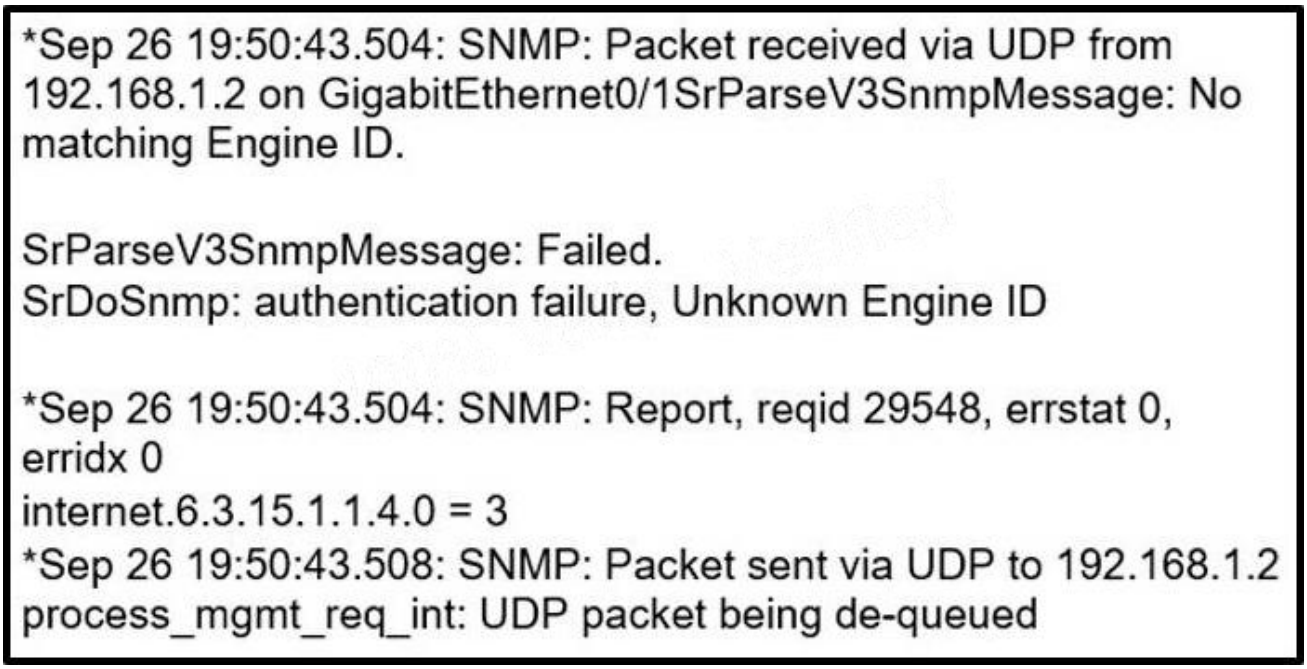
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book/ifindx.pdf

238.Refer to the exhibit.

```
*Sep 26 19:50:43.504: SNMP: Packet received via UDP from
192.168.1.2 on GigabitEthernet0/1SrParseV3SnmpMessage: No
matching Engine ID.

SrParseV3SnmpMessage: Failed.
SrDoSnmp: authentication failure, Unknown Engine ID

*Sep 26 19:50:43.504: SNMP: Report, reqid 29548, errstat 0,
erridx 0
internet.6.3.15.1.1.4.0 = 3
*Sep 26 19:50:43.508: SNMP: Packet sent via UDP to 192.168.1.2
process_mgmt_req_int: UDP packet being de-queued
```

Which two commands provide the administrator with the information needed to resolve the issue? (Choose two.)
A. Show snmp user
B. debug snmp engine-id
C. debug snmpv3 engine-id
D. debug snmp packet
E. showsnmpv3 user
Answer: A, D

239.Refer to the exhibit.



Which two commands provide the administrator with the information needed to resolve the issue? (Choose two.)

A. snmp user

B. debug snmp engine-id

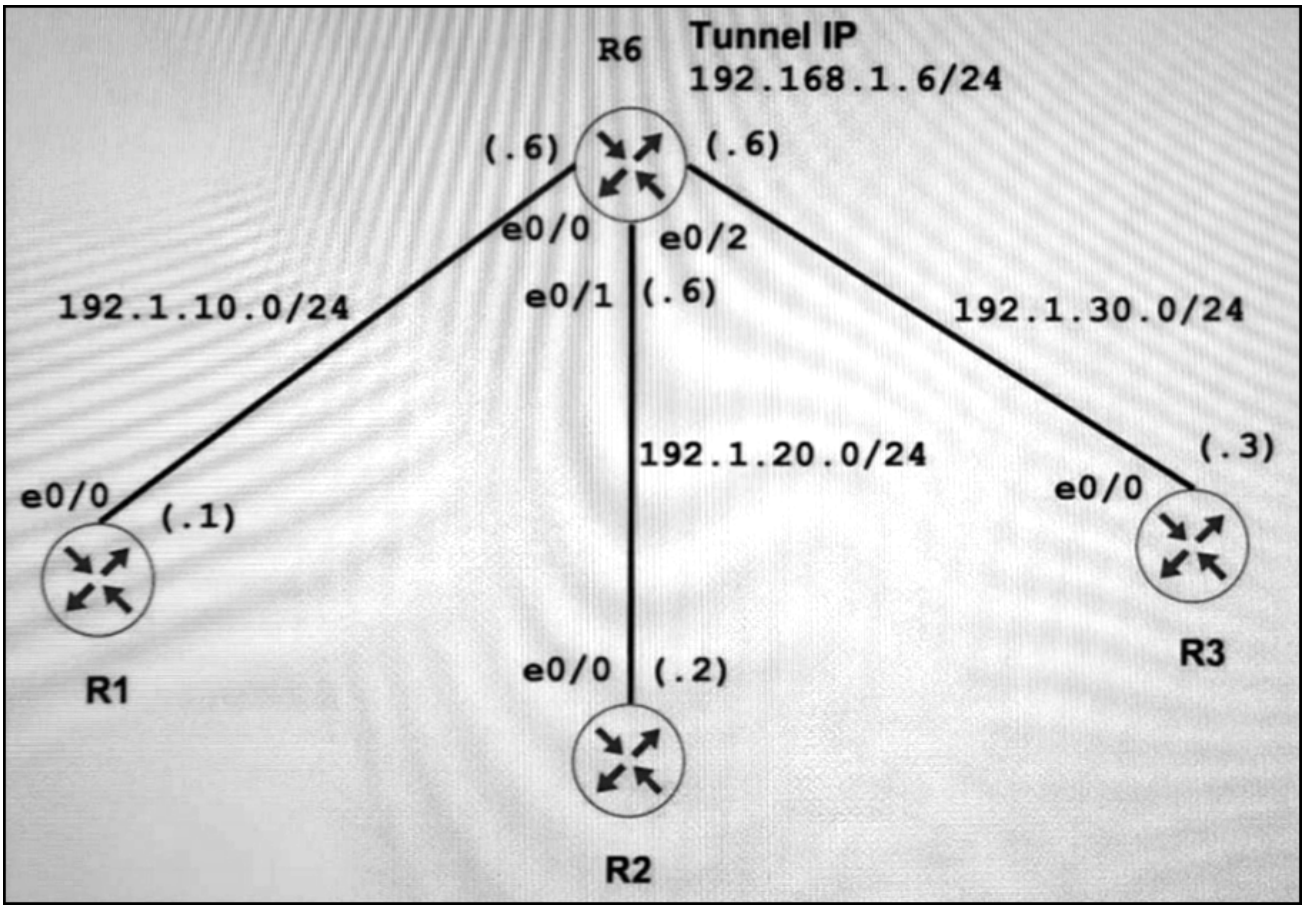
C. debug snmpv3 engine-id

D. debug snmp packet

E. showsnmpv3 user

Answer: A, E

240.Refer to the exhibit.



An engineer must establish multipoint GRE tunnels between hub router R6 and branch routers R1, R2, and R3.

Which configuration accomplishes this task on R1?

A)

```
interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source e0/1
 tunnel mode gre multipoint
 ip nhrp nhs 192.168.1.6
 ip nhrp map 192.168.1.6 192.1.10.6
```

B)

```
interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source e0/1
 tunnel mode gre multipoint
 ip nhrp network-id 1
 ip nhrp nhs 192.168.1.6
 ip nhrp map 192.168.1.6 192.1.10.1
 ip nhrp map 192.168.1.2 192.1.20.2
 ip nhrp map 192.168.1.3 192.1.30.3
```

C)

```
interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source e0/0
 tunnel mode gre multipoint
 ip nhrp nhs 192.168.1.6
 ip nhrp map 192.168.1.6 192.1.10.1
 ip nhrp map 192.168.1.2 192.1.20.2
 ip nhrp map 192.168.1.3 192.1.30.3
```

D)

```
interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source e0/0
 tunnel mode gre multipoint
 ip nhrp network-id 1
 ip nhrp nhs 192.168.1.6
 ip nhrp map 192.168.1.6 192.1.10.6
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

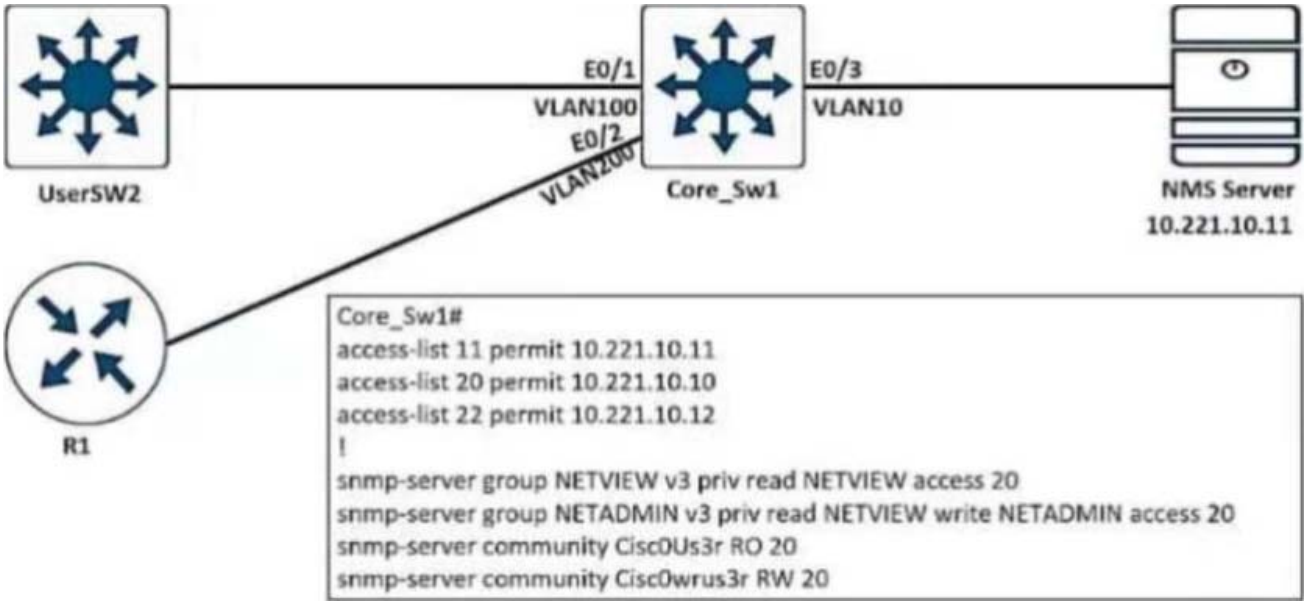
241.Refer to the exhibit.

```
interface loopback0
ip address 4.4.4.4 255.255.255.0
!
interface FastEthernet1/0
Description **** WAN link ****
ip address 10.0.0.1 255.255.2555.0
!
interface FastEthernet1/1
Description **** LAN Network ****
ip address 192.168.1.1 255.255.2555.0
!
!
router ospf 1
router-id 4.4.4.4
log-adjacency-changes
network 4.4.4.4 0.0.0.0 area 0
network 10.0.0.1 0.0.0.0 area 0
network 192.168.1.1 0.0.0.0 area 10
!
```

Which set of commands restore reachability to loopback0?

A. interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf network point-to-point
B. interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf network broadcast
C. interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf interface area 10
D. interface loopback0
ip address 4.4.4.4 255.255.255.0
ip ospf interface type network
Answer: A

242.Refer to the exhibit.



An engineer configured SNMP communities on the Core_SW1, but the SNMP server cannot obtain information from Core_SW1.
Which configuration resolves this issue?
A. snmp-server group NETVIEW v2c priv read NETVIEW access 20
B. access-list 20 permit 10.221.10.11
C. access-list 20 permit 10.221.10.12
D. snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22
Answer: B

243.What is a characteristic of Layer 3 MPLS VPNs?
A. LSP signaling requires the use of unnumbered IP links for traffic engineering.
B. Traffic engineering supports multiple IGP instances
C. Traffic engineering capabilities provide QoS and SLAs.
D. Authentication is performed by using digital certificates or preshared keys.

Answer: C

Explanation:

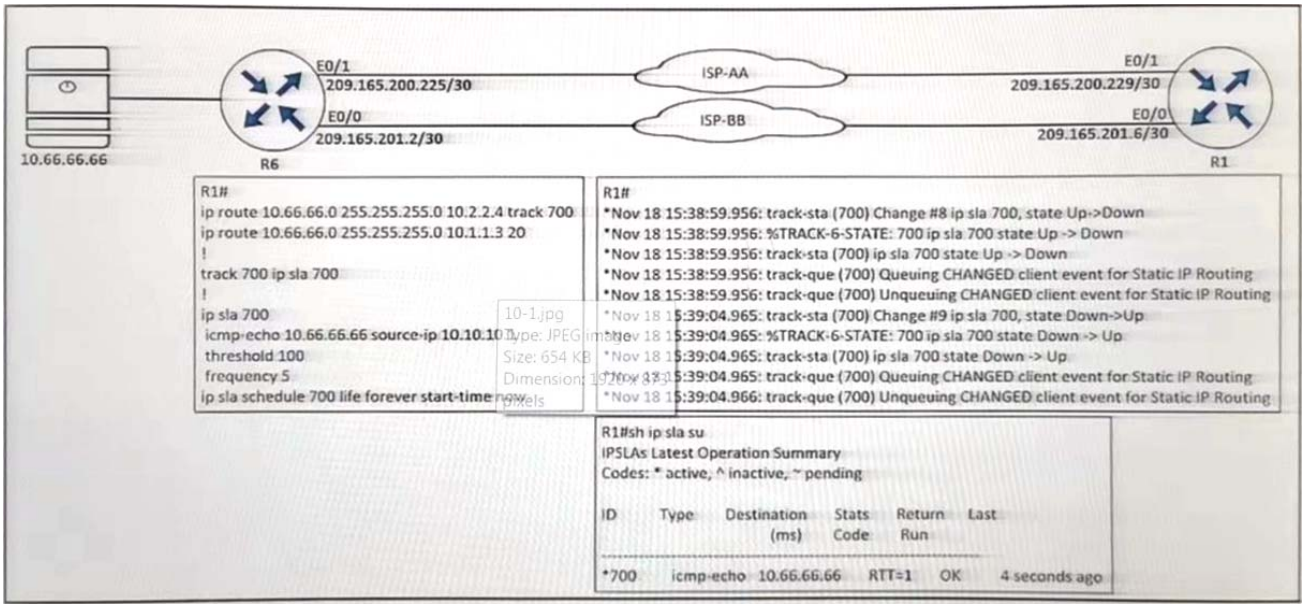
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_te_diffserv/configuration/15-mt/mp-te-diffserv-15-mt-book/mp-te-diffserv-aw.html

MPLS traffic engineering supports only a single IGP process/instance

The MPLS traffic engineering feature does not support routing and signaling of LSPs over unnumbered IP links.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_te_path_setup/configuration/xe-3s/mp-te-path-setup-xe-3s-book/mp-te-enhance-xe.html

244.Refer to the exhibit.



An engineer configured IP SLA on R1 to avoid the ISP link flapping problem. but it is not working as designed IP SLA should wait 30 seconds before switching traffic to a secondary connection and then revert to the primary link after waning 20 seconds, when the primary link is available and stabilized.

Which configuration resolves the issue?

A. R1(config)#ip sla 700
R1(config-ip-sla)#delay down 30 up 20

B. R1(config)#ip sla 700
R1(config-ip-sla)#delay down 20 up 30

C. R1(config)#track 700 ip sla 700
R1(config-track)#delay down 30 up 20

D. R1(config)#track 700 ip sla 700
R1(config-track)#delay down 20 up 30

Answer: C

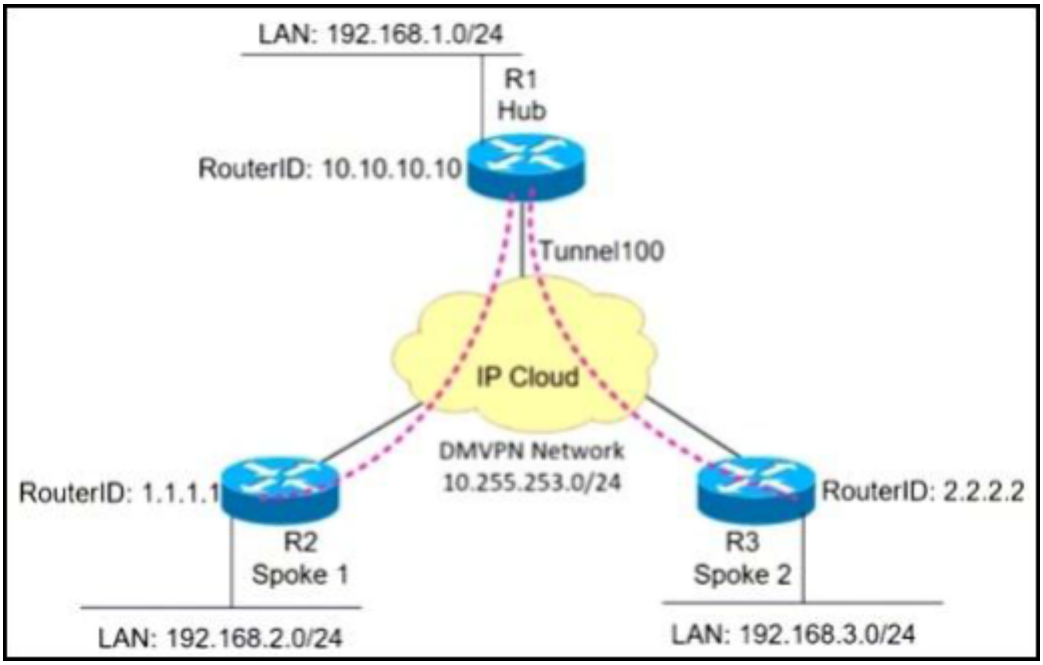
Explanation:

“wait 30 seconds before switching traffic to a secondary connection” -> delay down 30

“then revert to the primary link after waiting 20 seconds” -> up 20

Under the track object, you can specify delays so we have to configure delay under “track 700 ip sla 700” (not under “ip sla 700”).

245.Refer to the exhibit.




```
*Mar 1 17:19:04.051: %OSPF-5-ADJCHG: Process 100, Nbr 1.1.1.1 on Tunnel100 from LOADING to FULL, Loading Done
*Mar 1 17:19:06.375: %OSPF-5-ADJCHG: Process 100, Nbr 1.1.1.1 on Tunnel100 from FULL to DOWN, Neighbor Down: Adjacency forced to reset
*Mar 1 17:19:06.627: %OSPF-5-ADJCHG: Process 100, Nbr 2.2.2.2 on Tunnel100 from LOADING to FULL, Loading Done
*Mar 1 17:19:10.123: %OSPF-5-ADJCHG: Process 100, Nbr 2.2.2.2 on Tunnel100 from FULL to DOWN, Neighbor Down: Adjacency forced to reset
*Mar 1 17:19:14.499: %OSPF-5-ADJCHG: Process 100, Nbr 10.10.10.10 on Tunnel100 from LOADING to FULL, Loading Done
*Mar 1 17:19:19.139: %OSPF-5-ADJCHG: Process 100, Nbr 10.10.10.10 on Tunnel100 from EXSTART to DOWN, Neighbor Down: Interface down or detached
*Mar 1 17:01:51.975: %OSPF-4-NONEIGHBOR: Received database description from unknown neighbor 192.168.1.1
*Mar 1 17:01:57.783: OSPF: Rcv LS UPD from 192.168.1.1 on Tunnel100 length 88 LSA count 1
*Mar 1 17:01:57.155: OSPF: Send UPD to 10.255.253.1 on Tunnel100 length 100 LSA count 2
```

A network administrator sets up an OSPF routing protocol for a DMVPN network on the hub router.
Which configuration required to establish a DMVPN tunnel with multiple spokes?

A. ip ospf network point-to-multipoint on both spoke routers

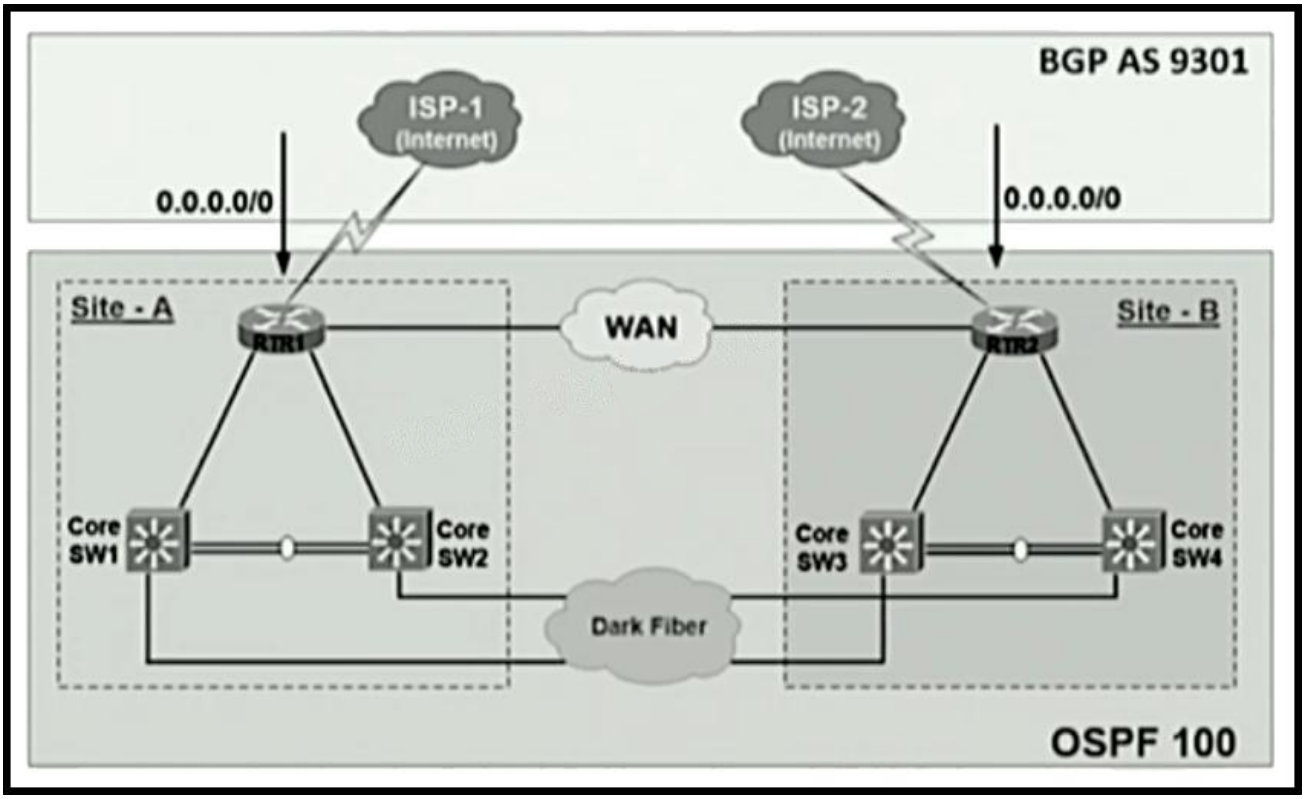
B. ip ospf network point-to-point on the hub router

C. ip ospf network point-to-multipoint on One spoke router

D. ip ospf network point-to-point on both spoke routers

Answer: A

246.Refer to the exhibit.



The Internet traffic should always prefer Site-A ISP-1 if the link and BGP connection are up; otherwise, all Internet traffic should go to ISP-2 Redistribution is configured between BGP and OSPF routing protocols and it is not working as expected.

What action resolves the issue?

A. Set metric-type 2 at Site-A RTR1, and set metric-type 1 at Site-B RTR2

B. Set OSPF cost 100 at Site-A RTR1, and set OSPF Cost 200 at Site-B RTR2

C. Set OSPF cost 200 at Site: A RTR1 and set OSPF Cost 100 at Site-B RTR2

D. Set metric-type 1 at Site-A RTR1, and set metric-type 2 at Site-B RTR2

Answer: D

Explanation:

OSPF type 1 route is always preferred over a type 2 route for the same destination so we can set metric-type 1 at Site-A RTR1 so that it is preferred over Site-B RTR2.

Note:

Routes are redistributed in OSPF as either type 1 (E1) routes or type 2 (E2) routes, with type 2 being the default.

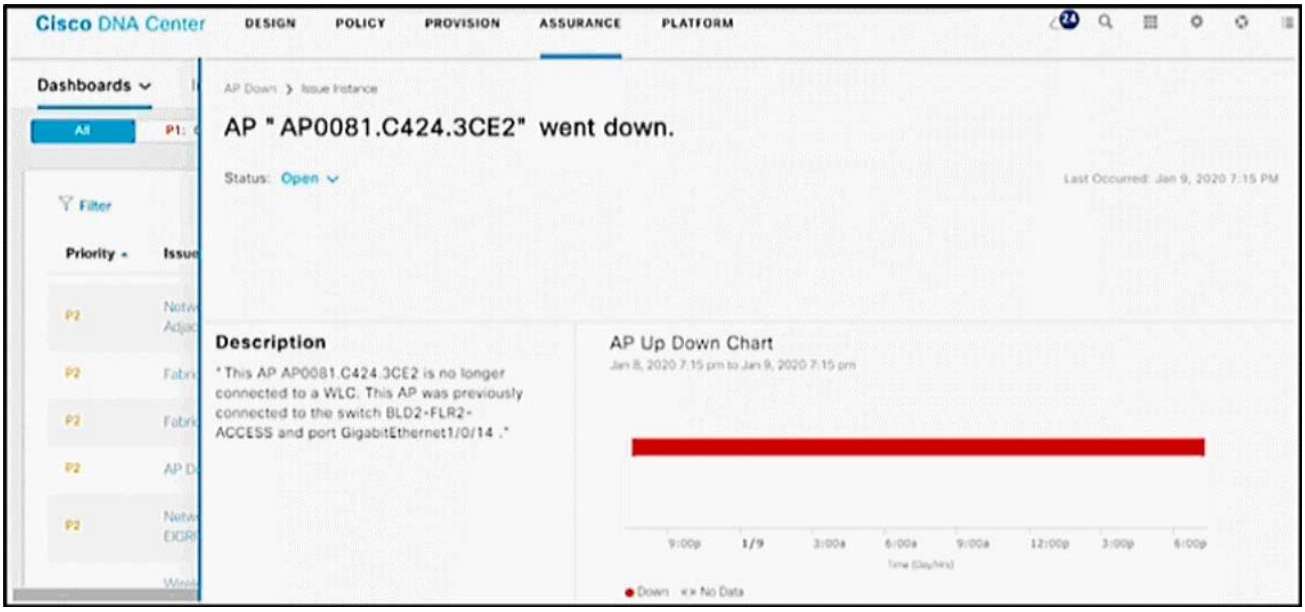
– A type 1 route has a metric that is the sum of the internal OSPF cost and the external redistributed cost.

– A type 2 route has a metric equal only to the redistributed cost.

– If routes are redistributed into OSPF as type 2 then every router in the OSPF domain will see the same cost to reach the external networks.

– If routes are redistributed into OSPF as type 1, then the cost to reach the external networks could vary from router to router.

247.Refer to the exhibit.



The AP status from Cisco DNA Center Assurance Dashboard shows some physical connectivity issues from access switch interface G1/0/14.

Which command generates the diagnostic data to resolve the physical connectivity issues?

A. test cable diagnostics tdr interface GigabitEthernet1/0/14

B. Check cable-diagnostics tdr interface GigabitEthernet1/0/14

C. show cable-diagnostics tdr interface GigabitEthernet1/0/14

D. Verify cable-diagnostics tdr interface GigabitEthernet1/0/14

Answer: A

Explanation:

The Time Domain Reflectometer (TDR) feature allows you to determine if a cable is OPEN or SHORT when it is at fault.

To start the TDR test, perform this task:

Step 1 (Starts the TDR test): test cable-diagnostics tdr {interface {interface-number}}

Step 2 (Displays the TDR test counter information): show cable-diagnostics tdr {interface interface-number}

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/16-11/configuration_guide/int_hw/b_1611_int_and_hw_9600_cg/checking_port_status_and_connectivity.pdf

```
TDR test started on interface Gi1/0/14
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

Wait 10 seconds and then issue the command to show the cable diagnostics result:

```
TDR test last run on: December 05 18:50:53
Interface Speed Local pair Pair length Remote pair Pair status
Gi1/0/14 1000M Pair A 19 +/- 10 meters Pair B Normal
               Pair B 19 +/- 10 meters Pair A Normal
               Pair C 19 +/- 10 meters Pair D Normal
               Pair D 19 +/- 10 meters Pair C Normal
```

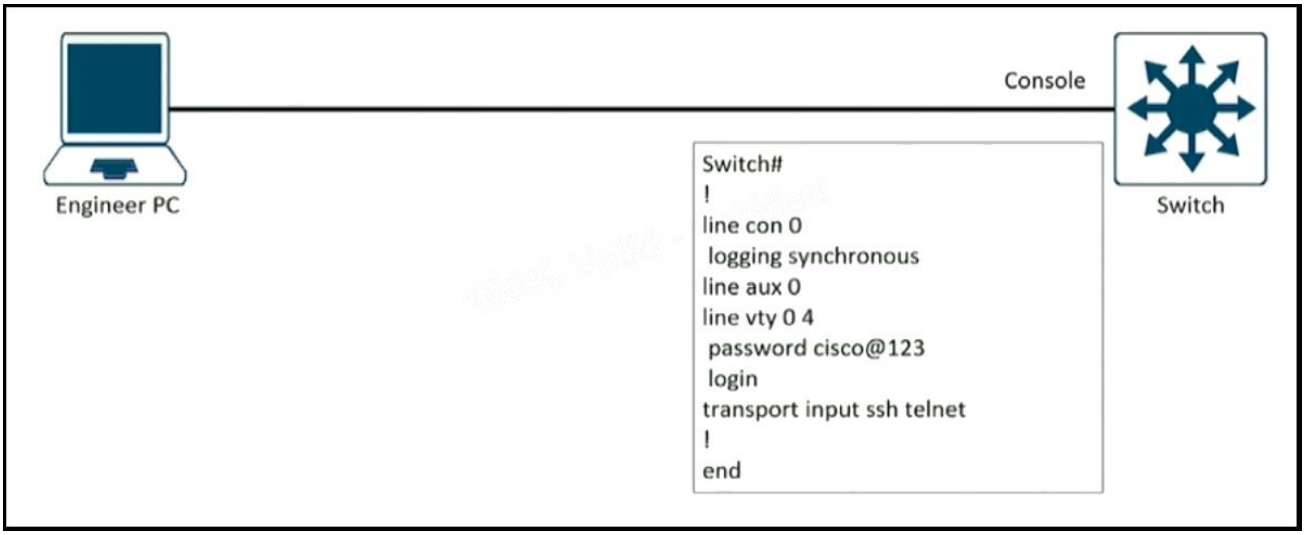
Notice that the results are "Normal" in the above example. Other results can be:
+ Open: Open circuit. This means that one (or more) pair has "no pin contact".
+ Short: Short circuit.
+ Impedance Mismatched: Bad cable.

248.An engineer creates a Cisco DNA Center cluster with three nodes, but all the services are running on one host node.
Which action resolves this issue?
A. Restore the link on the switch interface that is connected to a cluster link on the Cisco DNA Center
B. Click the master host node with all the services and select services to be moved to other hosts
C. Enable service distribution from the Systems 360 page.
D. Click system updates, and upgrade to the latest version of Cisco DNA Center.
Answer: C
Explanation:
To deploy Cisco DNA Center on a three-node cluster with High Availability (HA) enabled, complete the following procedure:
Step 1: Configure Cisco DNA Center on the first node in your cluster…
Step 2: Configure Cisco DNA Center on the second node in your cluster…
Step 3: Configure Cisco DNA Center on the third node in your cluster…
Step 4: Enable high availability on your cluster:
a. In the Cisco DNA Center GUI, click and choose System Settings. The System 360 tab is displayed by default.
b. In the Hosts area, click Enable Service Distribution.
After you click Enable Service Distribution, Cisco DNA Center enters into maintenance mode. In this mode, Cisco DNA Center is unavailable until the redistribution of services is completed. You should take this into account when scheduling an HA deployment.
Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automationand-management/dna-center/1-3-3-0/ha_guide/b_cisco_dna_center_ha_guide_1_3_3_0.html
Therefore we can choose "Enable Service Distribution" to distribute services to other host nodes.

249.R1 and R2 are configured as eBGP neighbor, R1 is in AS100 and R2 is in AS200.
R2 is advertising these networks to R1:

172.16.16.0/20
172.16.3.0/24
172.16.4.0/24
192.168.1.0/24
192.168.2.0/24
172.16.0.0/16
The network administrator on R1 must improve convergence by blocking all subnets of 172-16.0.0/16 major network with a mask lower than 23 from coming in.
Which set of configurations accomplishes the task on R1?
A. ip prefix-list PL-1 deny 172.16.0.0/16 le 23
ip prefix-list PL-1 permit 0.0.0.0/0 le 32
!
router bgp 100
neighbor 192.168.100.2 remote-as 200
neighbor 192.168.100.2 prefix-list PL-1 in
B. ip prefix-list PL-1 deny 172.16.0.0/16 ge 23
ip prefix-list PL-1 permit 0.0.0.0/0 le 32
!
router bgp 100
neighbor 192.168.100.2 remote-as 200
neighbor 192.168.100.2 prefix-list PL-1 in
C. access-list 1 deny 172.16.0.0 0.0.254.255
access-list 1 permit any
!
router bgp 100
neighbor 192.168.100.2 remote-as 200
neighbor 192.168.100.2 distribute-list 1 in
D. ip prefix-list PL-1 deny 172.16.0.0/16
ip prefix-list PL-1 permit 0.0.0.0/0
!
router bgp 100
neighbor 192.168.100.2 remote-as 200
neighbor 192.168.100.2 prefix-list PL-1 in
Answer: A
Explanation:
“Blocking all subnets of 172.16.0.0/16 major network with a mask lower than 23 from coming in” would block 172.16.16.0/20.
The first prefix-list “ip prefix-list PL-1 deny 172.16.0.0/16 le 23” means “all networks that fall within the 172.16.0.0/16 range AND that have a subnet mask of /23 or less” are denied.
The second prefix-list “ip prefix-list PL-1 permit 0.0.0.0/0 le 32” means allows all other prefixes.

250.Refer to the exhibit.



An engineer must block access to the console ports for all corporate remote Cisco devices based on the recent corporate security policy but the security team stilt can connect through the console port.
Which configuration on the console port resolves the issue?

A. transport input telnet
B. login and password
C. no exec
D. exec 0.0

Answer: C

Explanation:

“no exec” will disable access to a line. It is used if we want to allow only outgoing session (and disable incoming session) so this command will block all console port access.
There is no “exec 0 0” command. We can only find the “exec prompt” command in IOS Version 15.4(2)T4.

```
Router(config-line)#exec ?
  prompt  EXEC prompt
  <cr>

Router(config-line)#exec pro
Router(config-line)#exec prompt ?
  timestamp  Print timestamps for show commands

Router(config-line)#exec prompt
```

The most similar command is “exec-timeout 0 0” command, which is used to prevent Telnet/SSH sessions from timing out.

251.The network administrator configured R1 to authenticate Telnet connections based on Cisco ISE using TACACS+. ISE has been configured with an IP address of 192.168.1.5 and with a network device pointing toward R1(192.168.1.1) with a shared secret password of Cisco123.

```
aaa new-model
!
tacacs server ISE1
 address ipv4 192.168.1.5
 key Cisco123
!
aaa group server tacacs+ TAC-SERV
 server name ISE1
!
aaa authentication login telnet group TAC-SERV
```

The administrator cannot authenticate to R1 based on ISE.
Which configuration fixes the issue?
A. ip tacacs-server host 192.168.1.5 key Cisco123
B. line vty 0 4
login authentication TAC-SERV
C. line vty 0 4
login authentication telnet
D. tacacs-server host 192.168.1.5 key Cisco123
Answer: C
Explanation:
The last command “aaa authentication login telnet group TAC-SERV” created the method list name telnet so we need to assign it to line vty.
Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200208-Configure-ISE-2-0-IOS-TACACS-Authentic.html

252.Refer to the exhibit.

```
aaa new-model
aaa group server radius RADIUS-SERVERS
aaa authentication login default group RADIUS-SERVERS local
aaa authentication enable default group RADIUS-SERVERS enable
aaa authorization exec default group RADIUS-SERVERS if-authenticated
aaa authorization network default group RADIUS-SERVERS if-authenticated
aaa accounting send stop-record authentication failure
aaa session-id common
!
line con 0
logging synchronous
stopbits 1
line vty 0 4
logging synchronous
transport input ssh
```

A network administrator successfully logs in to a switch using SSH from a (RADIUS server When the

network administrator uses a console port to access the switch the RADIUS server returns shell:priv-lvl=15'' and the switch asks to enter the enable command \ the command is entered, it gets rejected. Which command set is used to troubleshoot and reserve this issue?

A. line con 0
aaa authorization console
authorization exec
!
line vty 0 4
transport input ssh

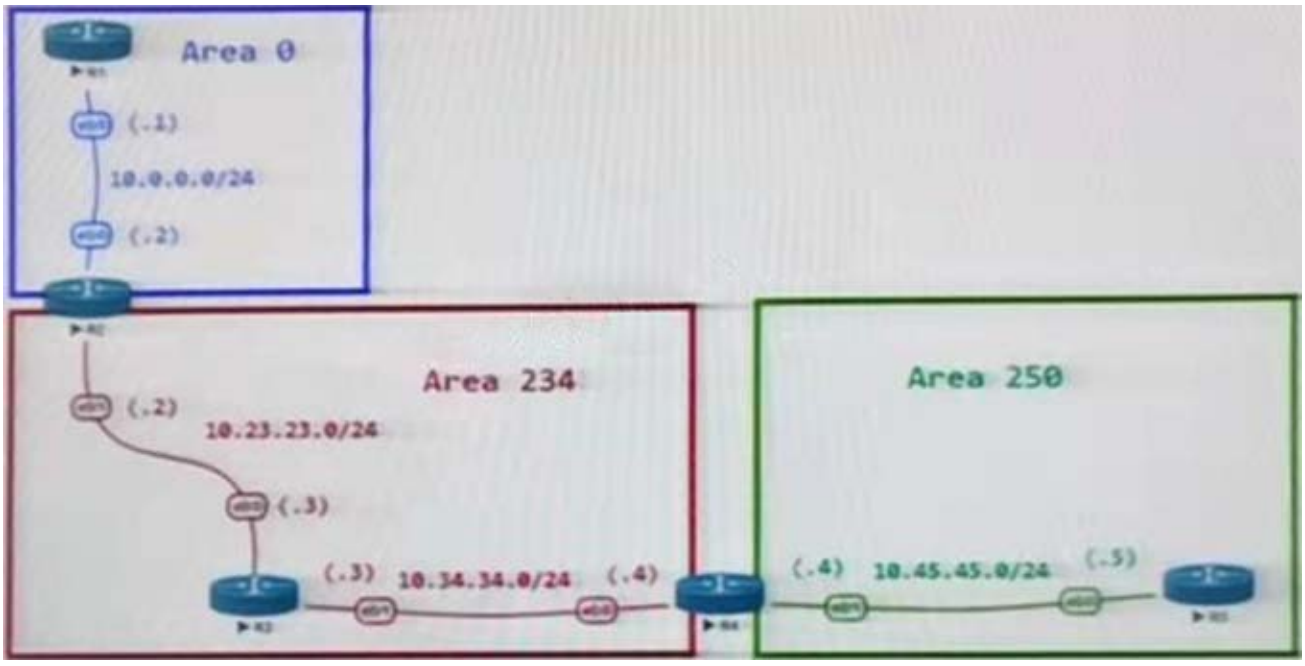
B. line con 0
aaa authorization console
!
line vty 0 4
authorization exec

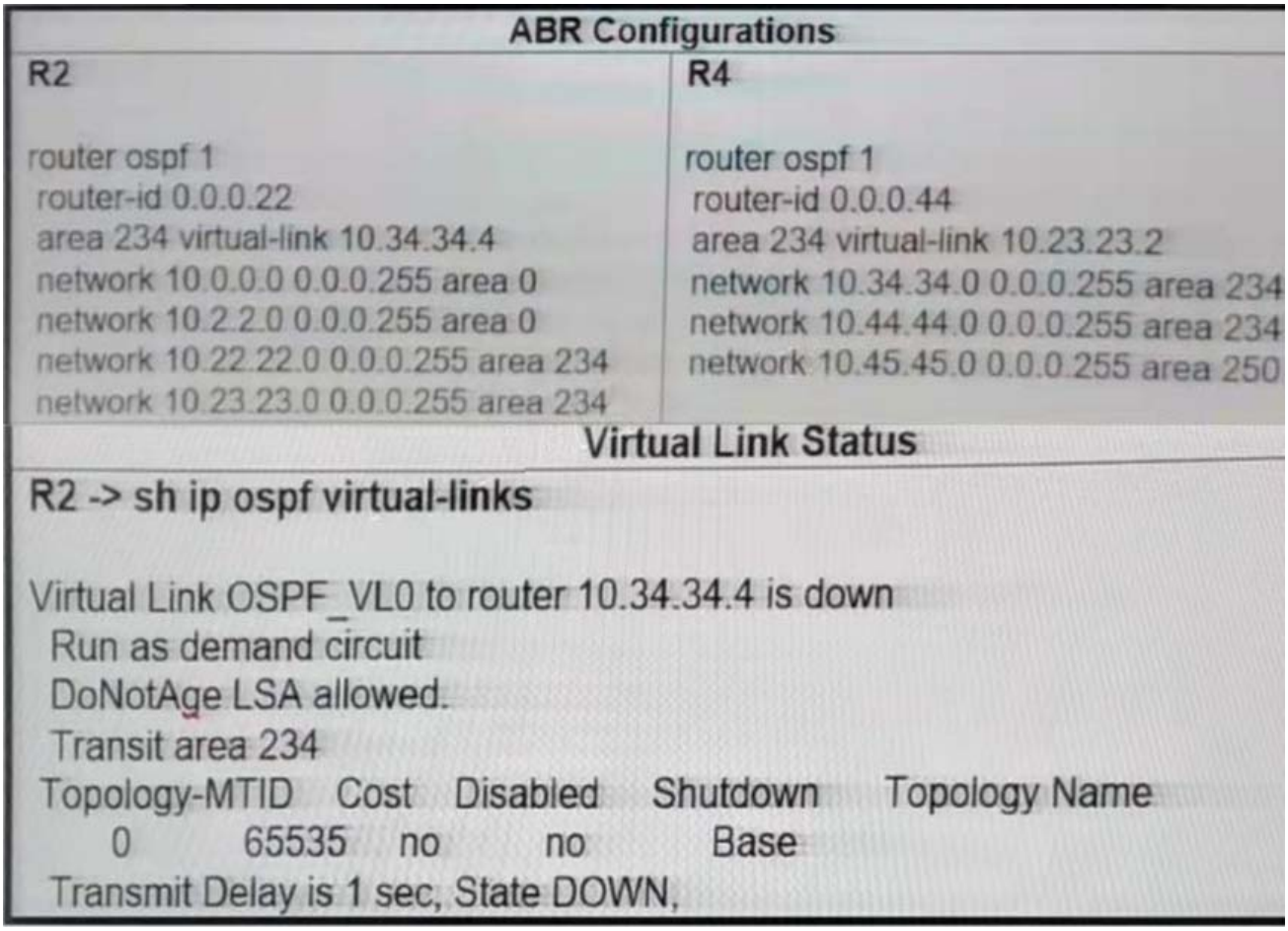
C. line con 0
aaa authorization console priv15
!
line vty 0 4
authorization exec

D. line con 0
aaa authorization console
authorization priv15
!
line vty 0 4
transport input ssh

Answer: A

253.Refer to the exhibit.





The network administrator configured the network to connect two disjointed networks and ail the connectivity is up except the virtual link which causes area 250 to be unreachable.
Which two configurations resolve this issue? (Choose two.)
A. R2
router ospf 1
router-id 10.23.23.2
B. R2
router ospf 1
no area area 234 virtual-link 10.34.34.4
area 0 virtual-link 0.0.0.44
C. R4
router ospf 1
no area 234 virtual-link 10.23.23.2
area 234 virtual-link 0.0.0.22
D. R2
router ospf 1
no area 234 virtual-link 10.34.34.4
area 234 virtual-link 0.0.0.44
E. R4
router ospf 1
no area area 234 virtual-link 10.23.23.2

area 0 virtual-link 0.0.0.22

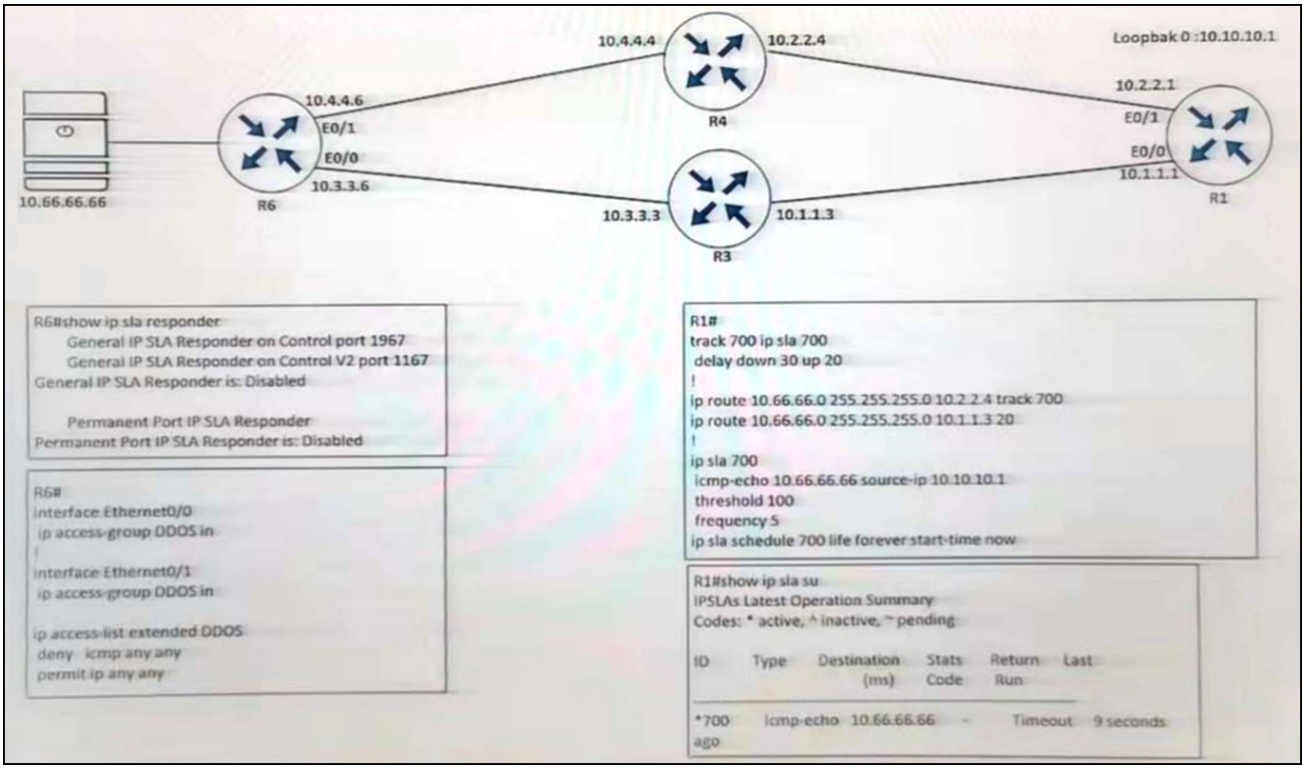
Answer: CD

Explanation:

Reference: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13703-8.html

An important thing to remember when configuring virtual-link is we need to configure the OSPF router ID and NOT the IP address of the ABR. Therefore in this question we have to use the command “area 234 virtual-link 0.0.0.44” on R2 and “area 234 virtual-link 0.0.0.22” on R4.

254.Refer to the exhibit.



R1 is configured with IP SLA to check the availability of the server behind R6 but it kept failing.

Which configuration resolves the issue?

A. R6(config)# ip sla responder

B. R6(config)# ip sla responder udp-echo ip address 10.10.10.1 port 5000

C. R6(config)# ip access-list extended DDOS

R6(config ext-nac)# 5 permit icmp host 10.66 66.66 host 10.10.10.1

D. R6(config)# ip access-list extended DDOS

R6(confg ext-nac)# 5 permit icmp host 10.10.10.1 host 10.66.66.66

Answer: D

Explanation:

In this IP SLA tracking, we don’t need a IP SLA Responder so the command “ip sla responder” on R6 is not necessary.

We also notice that the ACL is blocking ICMP packets on both interfaces E0/0 & E0/1 of R6 so we need to allow ICMP from source 10.10.10.1 to destination 10.66.66.66.

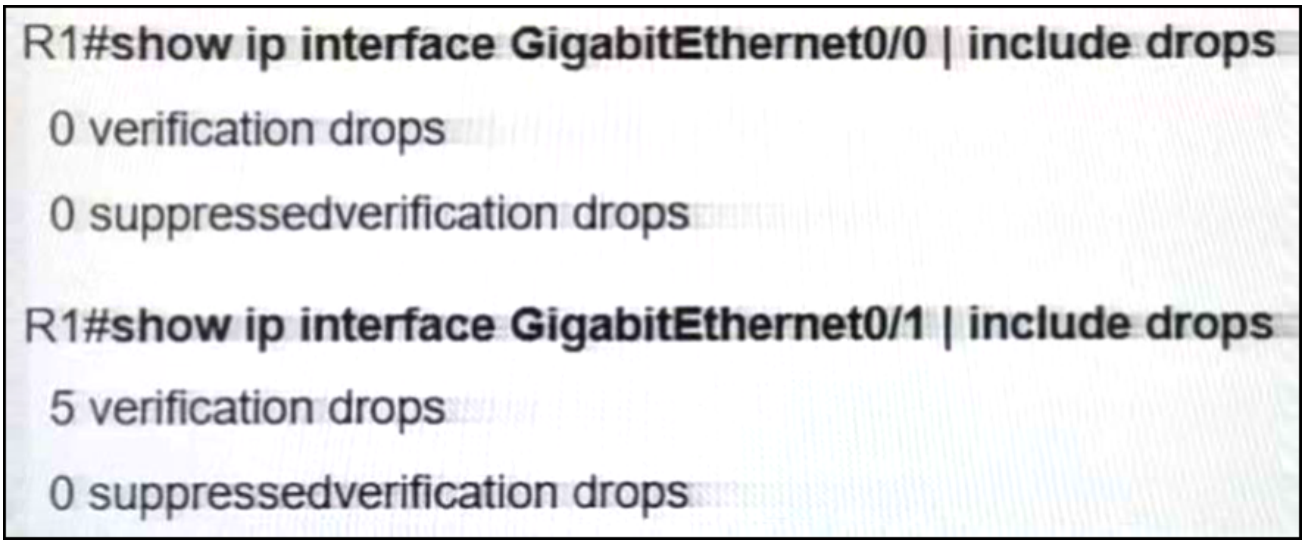
255.Which mechanism provides traffic segmentation within a DMVPN network?

A. RSVP
B. BGP
C. MPLS
D. iPsec
Answer: C
Explanation:
To use the DMPVN – Traffic Segmentation Within DMVPN feature you must configure Multiprotocol Label Switching (MPLS) by using the mpls ip command.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-16/sec-conn-dmvpn-xe-16-book/sec-conn-dmvpn-dmvpn.html

256.What are two characteristics of IPv6 Source Guard? (Choose two.)
A. requires IPv6 snooping on Layer 2 access or trunk ports
B. used in service provider deployments to protect DDoS attacks
C. requires the user to configure a static binding
D. requires that validate prefix be enabled
E. recovers missing binding table entries
Answer: DE
Explanation:
IPv6 Source Guard uses the IPv6 First-Hop Security Binding Table to drop traffic from unknown sources or bogus IPv6 addresses not in the binding table. The switch also tries to recover from lost address information, querying DHCPv6 server or using IPv6 neighbor discovery to verify the source IPv6 address after dropping the offending packet(s).
Reference: https://blog.ipspace.net/2013/07/first-hop-ipv6-security-features-in.html

257.How does an MPLS Layer 3 VPN differentiate the IP address space used between each VPN?
A. by RD
B. by address family
C. by MP-BGP
D. byRT
Answer: A

258.Refer to the exhibit.



R1 is configured with uRPF, and ping to R1 is failing from a source present in the R1 routing table via the GigatxtEthernet 0/0 interface.
Which action resolves the issue?
A. Remove the access list from the interface GigabrtEthernet 0/0
B. Modify the uRPF mode from strict to loose
C. Enable Cisco Express Forwarding to ensure that uRPF is functioning correctly
D. Add a floating static route to the source on R1 to the GigabitEthernet 0/1 interface
Answer: B

259.Which 0S1 model is used to insert an MPLS label?
A. between Layer 5 and Layer 6
B. between Layer 1 and Layer 2
C. between Layer 3 and Layer 4
D. between Layer 2 and Layer 3
Answer: D

260.Which function does LDP provide in an MPLS topology?
A. It enables a MPLS topology to connect multiple VPNs to P routers.
B. It provides hop-by-hop forwarding in an MPLS topology for LSRs.
C. It exchanges routes for MPLS VPNs across different VRFs.
D. It provides a means for LSRs to exchange IP routes.
Answer: B
Explanation:
LDP provides a standard methodology for hop-by-hop, or dynamic label, distribution in an MPLS network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting labeled paths, called label switch paths (LSPs), forward label traffic across an MPLS backbone to particular destinations.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/12-4t/mp-ldp-12-4t-book.pdf

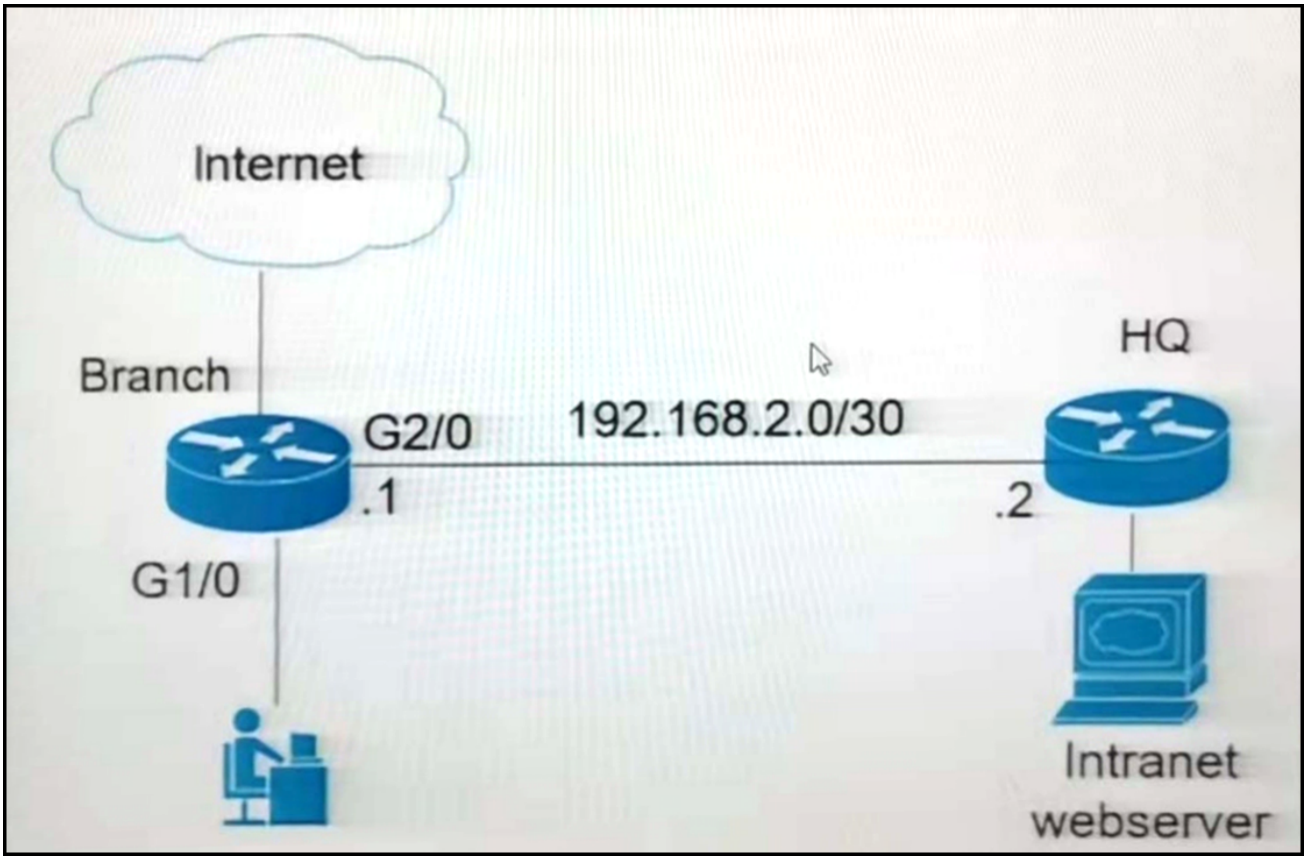
261.An engineer is implementing a coordinated change with a server team. As part of the change, the

engineer must configure interlace GigabitEthernet2 in an existing VRF "RED" then move the interface to an existing VRF "BLUE" when the server team is ready.
The engineer configured interface GigabitEthemet2 in VRF "RED"

```
interface GigabitEthernet2
description Migration ID: B410A60D0806G06
vrf forwarding RED
ip address 10.0.0.0 255.255.255.254
negotiation auto
```

Which configuration completes the change?
A. interface GigabitEthernet2
no ip address
vrf forwarding BLUE
B. interface GigabitEthernet2
no vrf forwarding RED
vrf forwarding BLUE
ip address 10.0.0.0 255.255.255.254
C. interface GigabitEthernet2
no vrf forwarding RED
vrf forwarding BLUE
D. interface GigabitEthernet2
no ip address
ip address 10.0.0.0 255.255.255.254
vrf forwarding BLUE
Answer: B
Explanation:
When assigning an interface to a VRF, the IP address will be removed so we have to reassign the IP address to that interface.

262.Refer to the exhibit.



The branch router is configured with a default route toward the internet and has no routes configured for the HQ site that is connected through interface G2/0. The HQ router is fully configured and does not require changes.

Which configuration on the branch router makes the intranet website (TCP port 80) available to the branch office users?

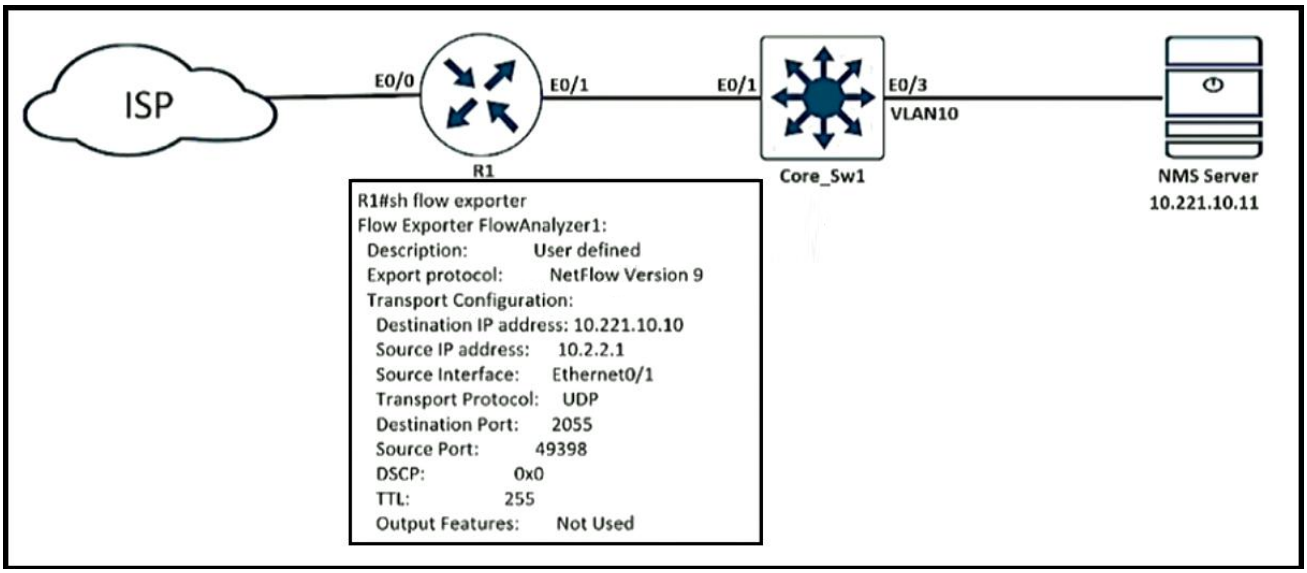
A. access-list 100 permit tcp any host intranet-webserver-ip eq 80
!
route-map pbr permit 10
match ip address 100
set ip next-hop 192.168.2.2
!
interface G2/0
ip policy route-map pbr

B. access-list 101 permit tcp any any eq 80
access-list 102 permit tcp any host intranet-webserver-ip
!
route-map pbr permit 10
match ip address 101 102
set ip next-hop 192.168.2.2
!
interface G1/0
ip policy route-map pbr

C. access-list 101 permit tcp any any eq 80

access-list 102 permit tcp any host intranet-webserver-ip
!
route-map pbr permit 10
match ip address 101
set ip next-hop 192.168.2.2
route-map pbr permit 20
match ip address 102
set ip next-hop 192.168.2 2
!
interface G2/0
ip policy route-map pbr
D. acceslist 100 permit tcp host intranet-webserverip eq 80 any
!
route-map pbr permit 10 match ip address 100
set ip next-hop 192.168 2.2
!
interface G1/0
ip policy route-map pbr
Answer: B
Explanation:
the ACL 101 matches all HTTP pakects while the ACL 102 matches TCP packets destined to Intranet webserver. These packets will be sent to HQ router.
If a match command refers to several objects in one command, either of them should match (the logical OR algorithm is applied). For example, in the match ip address 101 102 command, a route is permitted if it is permitted by access list 101 or access list 102.

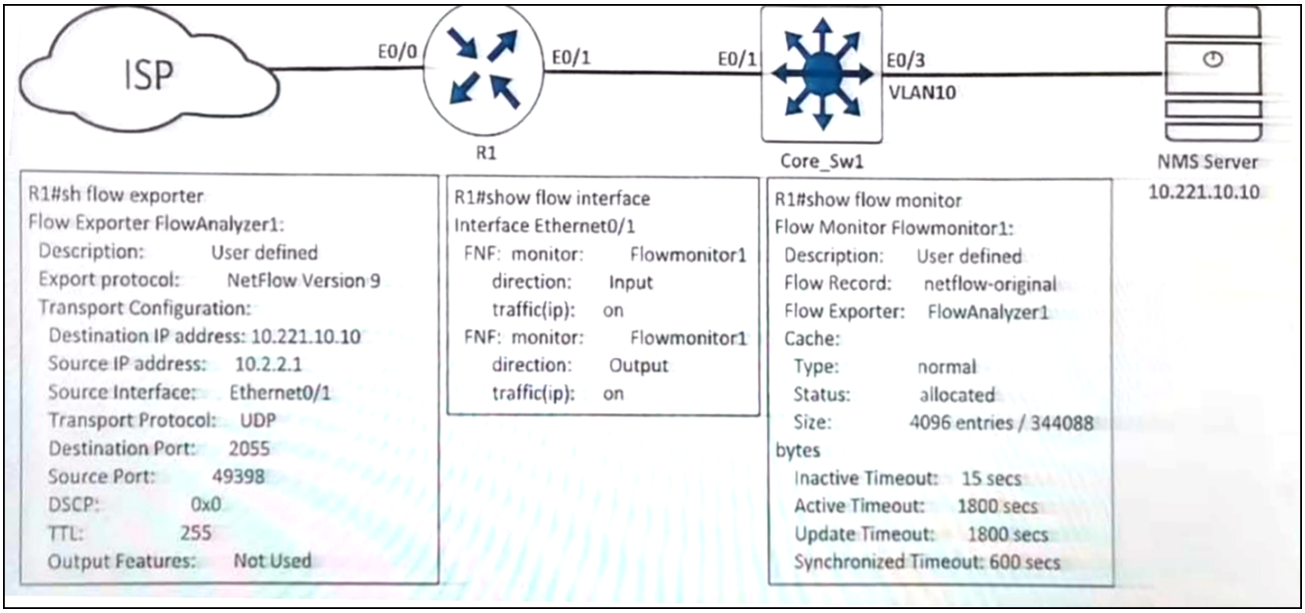
263.Refer to the exhibit.



An engineer configured NetFlow on R1, but the NMS server cannot see the flow from R1.
Which configuration resolves the issue?
A. flow monitor Flowmonitor1

destination 10.221.10.11
B. flow exporter FlowAnalyzer1
destination 10.221.10.11
C. interface Ethernet0/1
flow-destination 10.221.10.11
D. interface Ethernet0/0
flow-destination 10.221.10.11
Answer: B
Explanation:
From the output we notice that the destination IP address is not correct. The NMS server IP address should be 10.221.10.11, not 10.221.10.10. Therefore we have to change this information under “flow exporter …” configuration.
NetFlow configuration reference:
https://www.cisco.com/c/en/us/td/docs/iosxml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/cfg-de-fnflow-exprts.html

264.Refer to the exhibit.

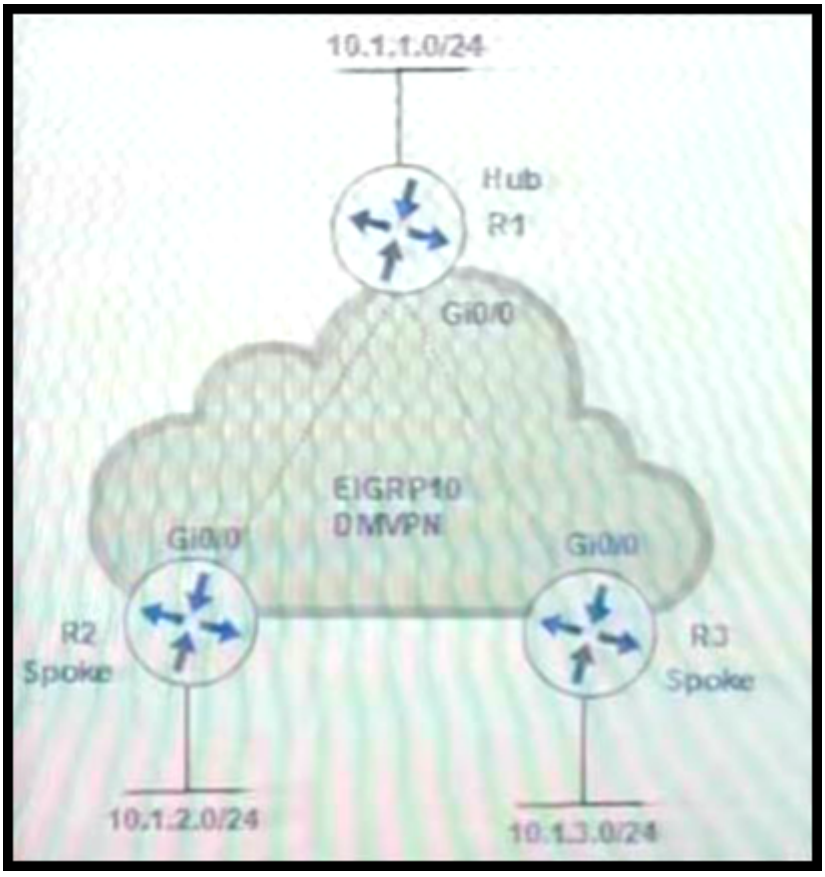


An engineer configured NetFlow on R1, but the NMS server cannot see the flow from ethernet 0/0 of R1.
Which configuration resolves the issue?
A. flow monitor Flowmonitor1
source Ethernet0/0
B. interface Ethernet0/1
ip flow monitor Flowmonitor1 input
ip flow monitor Flowmonitor1 output
C. interface Ethernet0/0
ip flow monitor Flowmonitor1 input
ip flow monitor Flowmonitor1 output
D. flow exporter FlowAnalyzer1
source Ethernet0/0

Answer: C

265.Refer to the exhibit.

```
R2#show ip route eigrp | include 10.1.
D      10.1.1.0/24

R3#show ip route eigrp | include 10.1.
D      10.1.1.0/24
```



An engineer configures DMVPN and receives the hub location prefix of 10.1.1.0724 on R2 and R3 The R3 prefix of 10 1.3.0/24 is not received on R2. and the R2 prefix 10.1,2.0/24 is not received on R3. Which action reserves the issue?

A. Split horizon prevents the routes from being advertised between spoke routers it should be disabled with the command no ip split-horizon eigrp 10 on the tunnel interface of R1

B. There is no spoke-to-spoke connection DMVPN configuration should be modified to enable a tunnel connection between R2 and R3 and neighbor relationship confirmed by use of the show ip eigrp neighbor command

C. Split horizon prevents the routes from being advertised between spoke routers it should be disabled with the no ip split-horizon eigrp 10 command on the Gi0/0 interface of R1.

D. There is no spoke-to-spoke connection DMVPN configuration should be modified with a manual

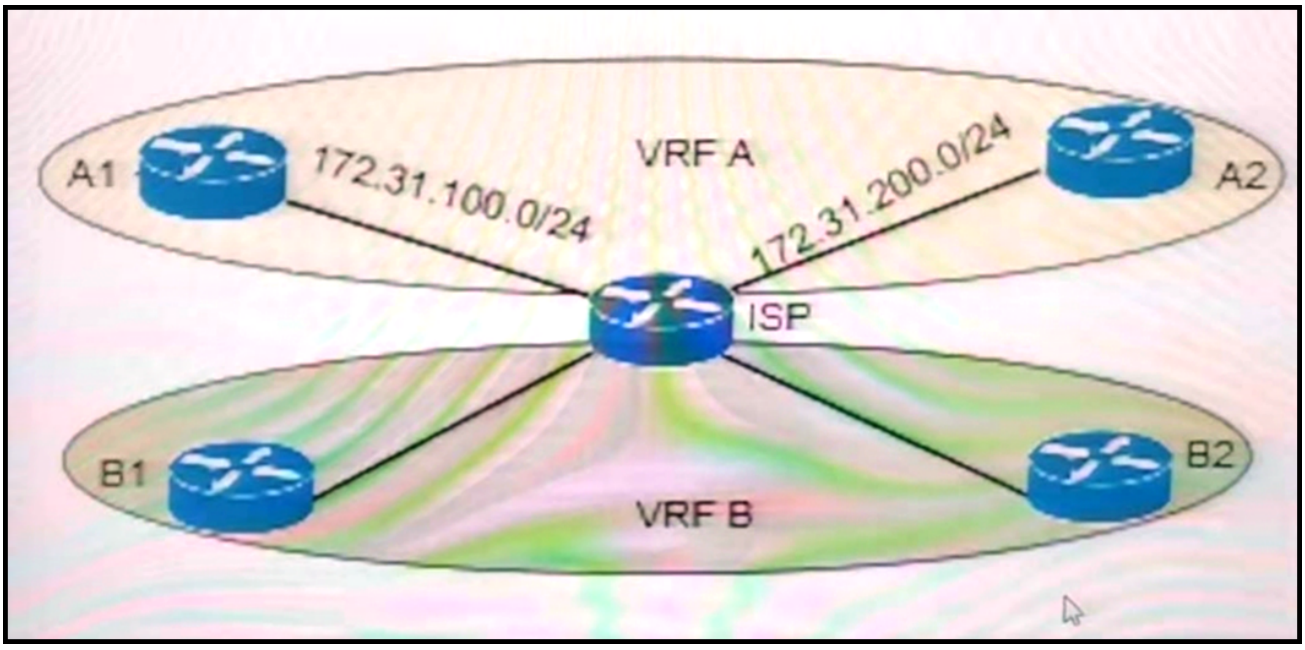
neighbor relationship configured between R2 and R3 and confirmed bb use of the show ip eigrp neighbor command.

Answer: A

Explanation:

In this topology, the Hub router will receive advertisements from R2 Spoke router on its tunnel interface. The problem here is that it also has a connection with R3 Spoke on that same tunnel interface. If we don't disable split-horizon, then the Hub will not relay routes from R2 to R3 and the other way around. That is because it received those routes on the same interface tunnel and therefore it cannot advertise back out that same interface (split-horizon rule). Therefore we must disable splithorizon on the Hub router to make sure the Spokes know about each other.

266.Refer to the exhibit.



The ISP router is fully configured for customer A and customer B using the VRF-Lite feature.

What is the minimum configuration required for customer A to communicate between routers A1 and A2?

A. A1

interface fa0/0

description To->ISP

ip add 172.31.100.1 255.255.255.0

no shut

!

router ospf 100

net 172.31.100.1 0.0.0.255 area 0

A2

interface fa0/0

description To->ISP

ip add 172.31.200.1 255.255.255.0

no shut

!

router ospf 100
net 172.31.200.1 0.0.0.255 area 0
B. A1
interface fa0/0
description To->ISP
ip vrf forwarding A
ip add 172.31.100.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.100.1 0.0.0.255 area 0
A2
interface fa0/0
description To->ISP
ip vrf forwarding A
ip add 172.31.200.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.200.1 0.0.0.255 area 0
C. A1
interface fa0/0
description To->ISP
ip add 172.31.200.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.200.1 0.0.0.255 area 0
A2
interface fa0/0
description To->ISP
ip add 172.31.100.1 255.255.255.0
no shut
!
router ospf 100
net 172.31.100.1 0.0.0.255 area 0
D. A1
interface fa0/0
description To->ISP
ip vrf forwarding A
ip add 172.31.100.1 255.255.255.0
no shut
!
router ospf 100 vrf A

net 172.31.200.1 0.0.0.255 area 0
A2
interface fa0/0
description To->ISP
ip vrf forwarding A
ip add 172.31.100.1 255.255.255.0
no shut
!
router ospf 100 vrf A
net 172.31.200.1 0.0.0.255 area 0
Answer: C
Explanation:
A1 and A2 routers do not know they belong to VRF
A. The two
interfaces of ISP (which are connected to A1 & A2) should be configured like this (we only show the configure of one interface):
ISP router:
interface g0/0
description ISP->To_CustomerA
ip vrf forwarding A
ip address 172.31.100.2 255.255.255.0
router ospf 100 vrf A
network 172.31.200.2 0.0.0.255 area 0

267.The network administrator configured R1 for Control Plane Policing so that the inbound Telnet traffic is policed to 100 kbps. This policy must not apply to traffic coming in from 10.1.1.1/32 and 172.16.1.1/32. The administrator has configured this:

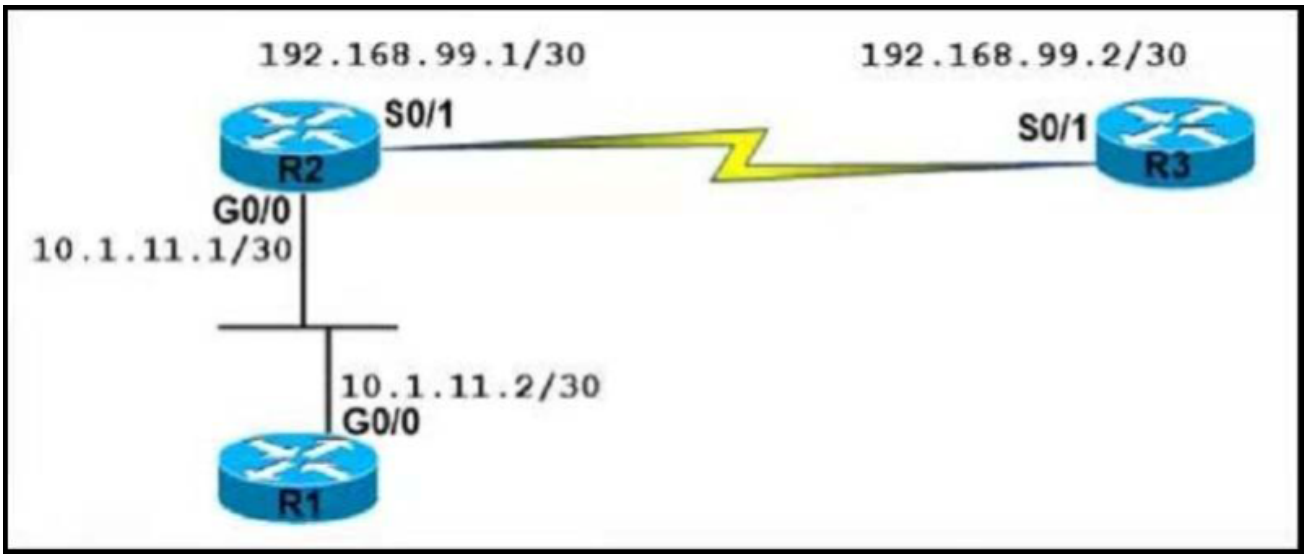
```
access-list 101 permit tcp host 10.1.1.1 any eq 23
access-list 101 permit tcp host 172.16.1.1 any eq 23
!
class-map CoPP-TELNET
match access-group 101
!
policy-map PM-CoPP
class CoPP-TELNET
police 100000 conform transmit exceed drop
!
control-plane
service-policy input PM-CoPP
```

The network administrator is not getting the desired results.
Which set of configurations resolves this issue?

A. control-plane
no service-policy input PM-CoPP
!
interface Ethernet 0/0
service-policy input PM-CoPP
B. control-plane
no service-policy input PM-CoPP
service-policy input PM-CoPP
C. no access-list 101
access-list 101 deny tcp host 10,1,1.1 any eq 23
access-list 101 deny tcp host 172,16.1.1 any eq 23
access-list 101 permit ip any any
D. no access-list 101
access-list 101 deny tcp host 10,1.1.1 any eq 23
access-list 101 deny tcp host 172.16.1.1 any eq 23
access-list 101 permit ip any any
!
interface E0/0
service-policy input PM-CoPP
Answer: C
Explanation:
Packets that match a deny rule are excluded from that class and cascade to the next class (if one exists) for classification. Therefore if we don't want to CoPP traffic from 10.1.1.1/32 and 172.16.1.1/32, we must "deny" them in the ACL.

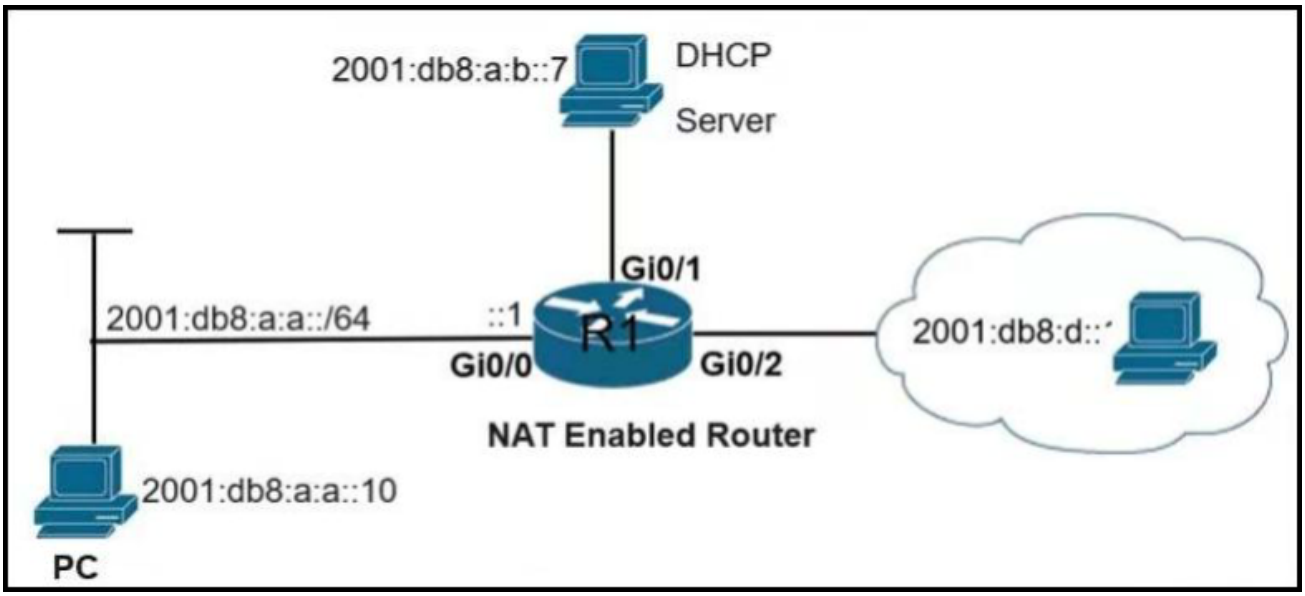
268.Refer to the exhibit.

```
R2# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.99.2      1   EXCHANGE/  -    00:00:36    192.168.99.1    Serial0/1
router-6#

R3# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.99.1      1   EXSTART/  -     00:00:33    192.168.99.2    Serial0/1
```



An OSPF neighbor relationship between R2 and R3 is showing stuck in EXCHANGE/EXSTART state. The neighbor is established between R1 and R2. The network engineer can ping from R2 to R3 and vice versa, but the neighbor is still down.
Which action resolves the issue?
A. Restore the Layer 2/Layer 3 connectivity issue in the ISP network.
B. Match MTU on both router interfaces or ignore MTU.
C. Administrative "shut then no shut" both router interfaces.
D. Enable OSPF on the interface, which is required.
Answer: B
Explanation:
After two OSPF neighboring routers establish bi-directional communication and complete DR/BDR election (on multi-access networks), the routers transition to the exstart state. In this state, the neighboring routers establish a master/slave relationship and determine the initial database descriptor (DBD) sequence number to use while exchanging DBD packets.
Neighbors Stuck in Exstart/Exchange State
The problem occurs most frequently when attempting to run OSPF between a Cisco router and another vendor’s router. The problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces don’t match. If the router with the higher MTU sends a packet larger that the MTU set on the neighboring router, the neighboring router ignores the packet.

269.Refer to the exhibit.




```
C:\PC> ping 2001:db8:a:b::7
Pinging 2001:db8:a:b::7 with 32 bytes of data:
Reply from 2001:db8:a:b::7: time=46ms
Reply from 2001:db8:a:b::7: time=40ms
Reply from 2001:db8:a:b::7: time=40ms
Reply from 2001:db8:a:b::7: time=40ms
Ping statistics for 2001:db8:a:b::7:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 40ms, Maximum = 46ms, Average = 41ms

R1# telnet 2001:db8:a:b::7
Trying 2001:DB8:A:B::7 ... Open
User Access Verification
Password:

R1# show ipv6 access-list TSHOOT
IPv6 access list TSHOOT
deny tcp any host 2001:DB8:A:B::7 eq telnet (6 matches) sequence 10
permit tcp host 2001:DB8:A:A::10 host 2001:DB8:A:B::7 eq telnet sequence 20
permit tcp host 2001:DB8:A:A::10 host 2001:DB8:D::1 eq www sequence 30
permit ipv6 2001:DB8:A:A::/64 any (67 matches) sequence 40
```

An engineer is troubleshooting a failed Telnet session from PC to the DHCP server.

Which action resolves the issue?

A. Remove sequence 30 and add it back to the IPv6 traffic filter as sequence 5.

B. Remove sequence 20 and add it back to the IPv6 traffic filter as sequence 5.

C. Remove sequence 10 to add the PC source IP address and add it back as sequence 10.

D. Remove sequence 20 for sequence 40 in the access list to allow Telnet.

Answer: B

270.Refer to the exhibit.

```
ip sla 1
 icmp-echo 8.8.8.8
 threshold 1000
 timeout 2000
 frequency 5
ip sla schedule 1 life forever start-time now
!
track 1 ip sla 1
!
ip route 0.0.0.0 0.0.0.0 203.0.113.1 name ISP1 track 1
ip route 0.0.0.0 0.0.0.0 198.51.100.1 2 name ISP2
```

The administrator noticed that the connection was flapping between the two ISPs instead of switching to ISP2 when the ISP1 failed.
Which action resolves the issue?
A. Include a valid source-interface keyword in the icmp-echo statement.
B. Reference the track object 1 on the default route through ISP2 instead of ISP1.
C. Modify the static routes to refer both to the next hop and the outgoing intertace.
D. Modify the threshold to match the administrative distance of the ISP2 route.
Answer: A
Explanation:
https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200785-ISP-Failover-withdefault-routes-using-I.html

271.Refer to the exhibit.

```
RR# show running-config
!
interface Ethernet0/1
 no ip address
 ipv6 address 2001:DB8:1:12::2/64
 ipv6 traffic-filter ACL in
!
ipv6 access-list ACL
 sequence 10 permit tcp any any eq 22
 sequence 20 permit tcp any eq 22 any
 sequence 30 permit tcp any any eq bgp
 sequence 40 permit tcp any eq bgp any
 sequence 50 permit udp any any eq ntp
 sequence 60 permit udp any eq ntp any
 sequence 70 permit udp any any eq snmp
 sequence 80 deny ipv6 any any log

RR# show ipv6 cef ::/0
::/0
  nexthop 2001:DB8:1:12::1 Ethernet0/1

*Feb 23 00:23:17.211: %IPV6_ACL-6-ACCESSLOGDP: list ACL/80
denied icmpv6 2001:DB8:1:12::1 -> FF02::1:FF00:2 (135/0), 7321
packets
```

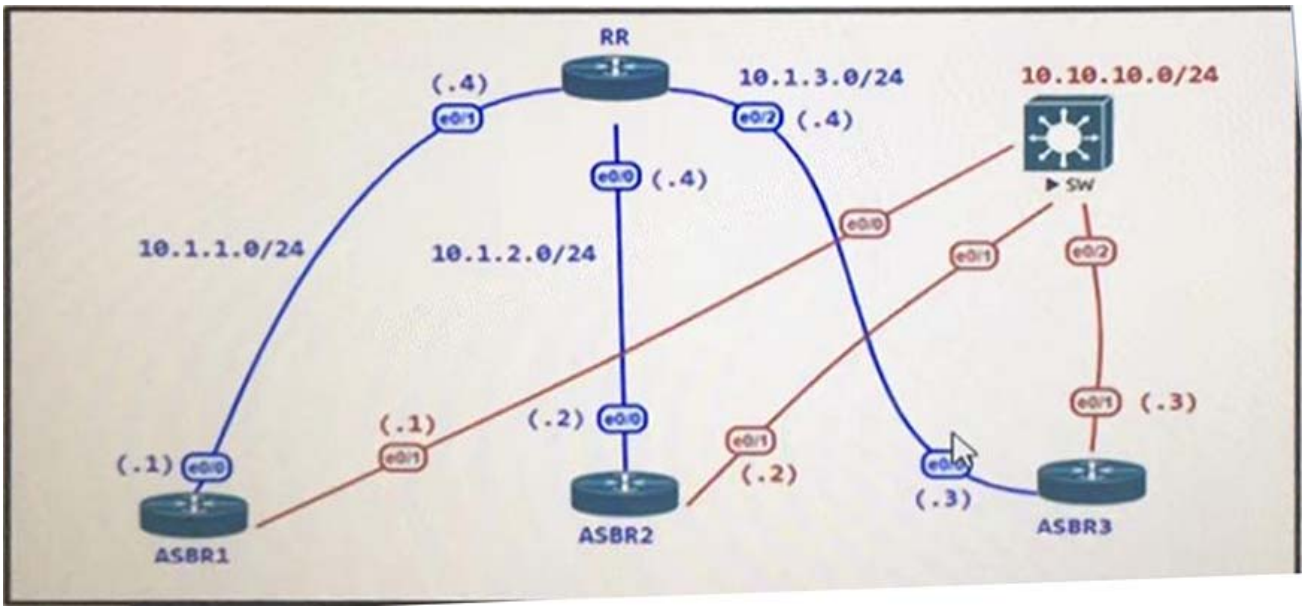
After a security audit, the administrator implemented an ACL in the route reflector. The RR became unreachable from any router in the network.
Which two actions resolve the issue? (Choose two.)
A. Enable the ND proxy feature on the default gateway.
B. Configure a link-local address on the Ethernet0/1 interface.
C. Permit ICMPv6 neighbor discovery traffic in the ACL.
D. Remove the ACL entry 80.
E. Change the next hop of the default route to the link-local address of the default gateway.
Answer: CD

272.Refer to the exhibit.

```
R1 (config)# ip vrf CCNP
R1 (config-vrf)# rd 1:100
R1 (config-vrf)# exit
R1 (config)# interface Loopback0
R1 (config-if)# ip address 10.1.1.1 255.255.255.0
R1 (config-if)# ip vrf forwarding CCNP
R1 (config-if)# exit
R1 (config)# exit
R1# ping vrf CCNP 10.1.1.1
% Unrecognized host or address, or protocol not running.
```

Which command must be configured to make VRF CCNP work?
A. interface Loopback0
vrf forwarding CCNP
B. interface Loopback0
ip address 10.1.1.1 255.255.255.0
C. interface Loopback0
ip address 10.1.1.1 255.255.255.0
vrf forwarding CCNP
D. interface Loopback0
ip address 10.1.1.1 255.255.255.0
ip vrf forwarding CCNP
Answer: B
Explanation:
From the exhibit, we learn that the command “ip address 10.1.1.1 255.255.255.0” has been issued before the command “ip vrf forwarding CCNP”. But the second command removed the IP address configured in the first command so we have to retype the IP address command.

273.Refer to the exhibit.



RR

```
router bgp 100
 neighbor 10.1.1.1 remote-as 100
 neighbor 10.1.2.2 remote-as 100
 neighbor 10.1.3.3 remote-as 100
```

ASBR2

```
router bgp 100
 neighbor 10.1.1.4 remote-as 100
```

ASBR3

```
router bgp 100
 neighbor 10.1.2.4 remote-as 100
```

ASBR4

```
router bgp 100
 neighbor 10.1.3.4 remote-as 100
```

The administrator configured the network devise for end-to-end reachability, but the ASBRs are not propagation routes to each other.

Which set of configuration resolves this issue?
A. router bgp 100
neighbor 10.1.1.1 route-reflector-client
neighbor 10.1.2.2 route-reflector-client
neighbor 10.1.3.3 route-reflector-client
B. router bap 100
neighbor 10.1.1.1 next-hop-self
neighbor 10.1.2.2 next-hop-self
neighbor 10.1.3.3 next-hop-self
C. router bgp 100
neighbor 10.1.1.1 update-source Loopback0
neighbor 10.1.2.2 update-source Loopback0
neighbor 10.1.3.3 update-source Loopback0
D. router bgp 100
neighbor 10.1.1.1 ebgp-multihop
neighbor 10.1.2.2 ebgp-multihop
neighbor 10.1.3.3 ebgp-multihop
Answer: A

274.A company is expanding business by opening 35 branches over the Internet. A network engineer must configure DMVPN at the branch routers to connect with the hub router and allow NHRP to add spoke routers securely to the multicast NHRP mappings automatically.
Which configuration meets this requirement at the hub router?
A. interface Tunnel0
ip address 10.0.0.1 255.255.255.0
ip nhrp authentication KEY1
ip nhrp nhs dynamic
ip nhrp network-id 10
tunnel mode mgre auto
B. interface Tunne10
ip address 10.0.0.1 255.255.255.0
ip nhrp authentication KEY1
ip nhrp registration no-unique
ip nhrp network-id 10
tunnel mode gre nmba
C. interface Tunnel0
ip address 10.0.0.1 255.255.255.0
ip nhrp authentication KEY1
ip nhrp map multicast dynamic
ip nhrp network-id 10
tunnel mode gre multi pointe
D. interface Tunnel0
ip address 10.0.0.1 255.255.255.0
ip nhrp authentication KEY 1

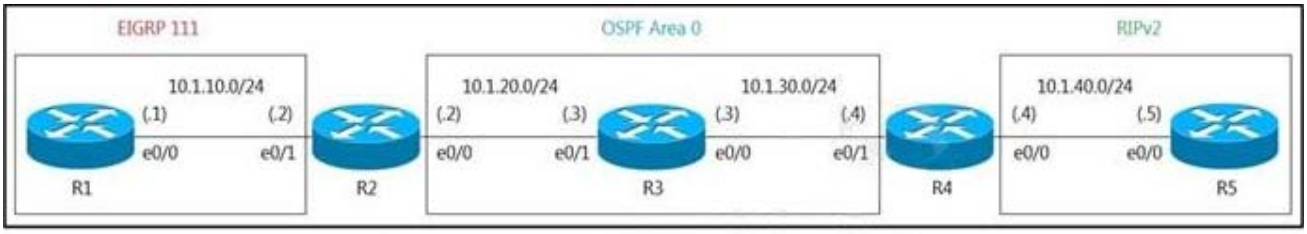
ip nhrp map multicast 224.0.0.0
ip nhrp network-id 10
tunnel mode gre ipv4
Answer: C
Explanation:
The command “ip nhrp map multicast dynamic” allows NHRP to automatically add spoke routers to the multicast NHRP mappings.

275.What is an advantage of implementing BFD?
A. BFD provides faster updates for any flapping route.
B. BFD provides millisecond failure detection
C. BFD is deployed without the need to run any routing protocol
D. BFD provides better capabilities to maintain the routing table
Answer: B

276.What is a function of IPv6 Source Guard?
A. It works with address glean or ND to find existing addresses.
B. It inspects ND and DHCP packets to build an address binding table.
C. It denies traffic from known sources and allocated addresses.
D. It notifies the ND protocol to inform hosts if the traffic is denied by it.
Answer: A
Explanation:
IPv6 source guard is an interface feature between the populated binding table and data traffic filtering. This feature enables the device to deny traffic when it is originated from an address that is not stored in the binding table. IPv6 source guard does not inspect ND or DHCP packets; rather, it works in conjunction with IPv6 neighbor discovery (ND) inspection or IPv6 address glean, both of which detect existing addresses on the link and store them into the binding table.

277.What is the purpose of the DHCPv6 Guard?
A. It messages between a DHCPv6 server and a DHCPv6 client (or relay agent).
B. It shows that clients of a DHCPv5 server are affected.
C. It block DHCPv6 messages from relay agents to a DHCPv6 server.
D. It allows DHCPv6 replay and advertisements from (rouge) DHCPv6 servers.
Answer: A
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16/ip6fxe-16-book/ip6-dhcpv6-guard.html

278.Refer to the exhibit.




```
R2
route-map E20 permit 10
 set tag 111
!
router eigrp 111
 redistribute ospf 1 metric 10 10 10 10 10
!
router ospf 1
 redistribute eigrp 111 route-map E20 subnets

R4
router rip
router ospf 1
 redistribute rip subnets
```

R5 should not receive any routes originated in the EIGRP domain.
Which set of configuration changes removes the EIGRP routes from the R5 routing table to fix the issue?
A. R4
route-map O2R deny 10
match tag 111
route-map O2R permit 20
!
router rip
redistribute ospf 1 route-map O2R metric 1
B. R2
route-map E20 deny 20
R4
route-map O2R deny 10
match tag 111
!
router rip
redistribute ospf 1 route-map O2R metric 1
C. R4
route-map O2R permit 10
match tag 111
route-map O2R deny 20
!
router rip
redistribute ospf 1 route-map O2R metric 1
D. R4
route-map O2R deny 10
match tag 111
!
router rip

redistribute ospf 1 route-map O2R metric 1

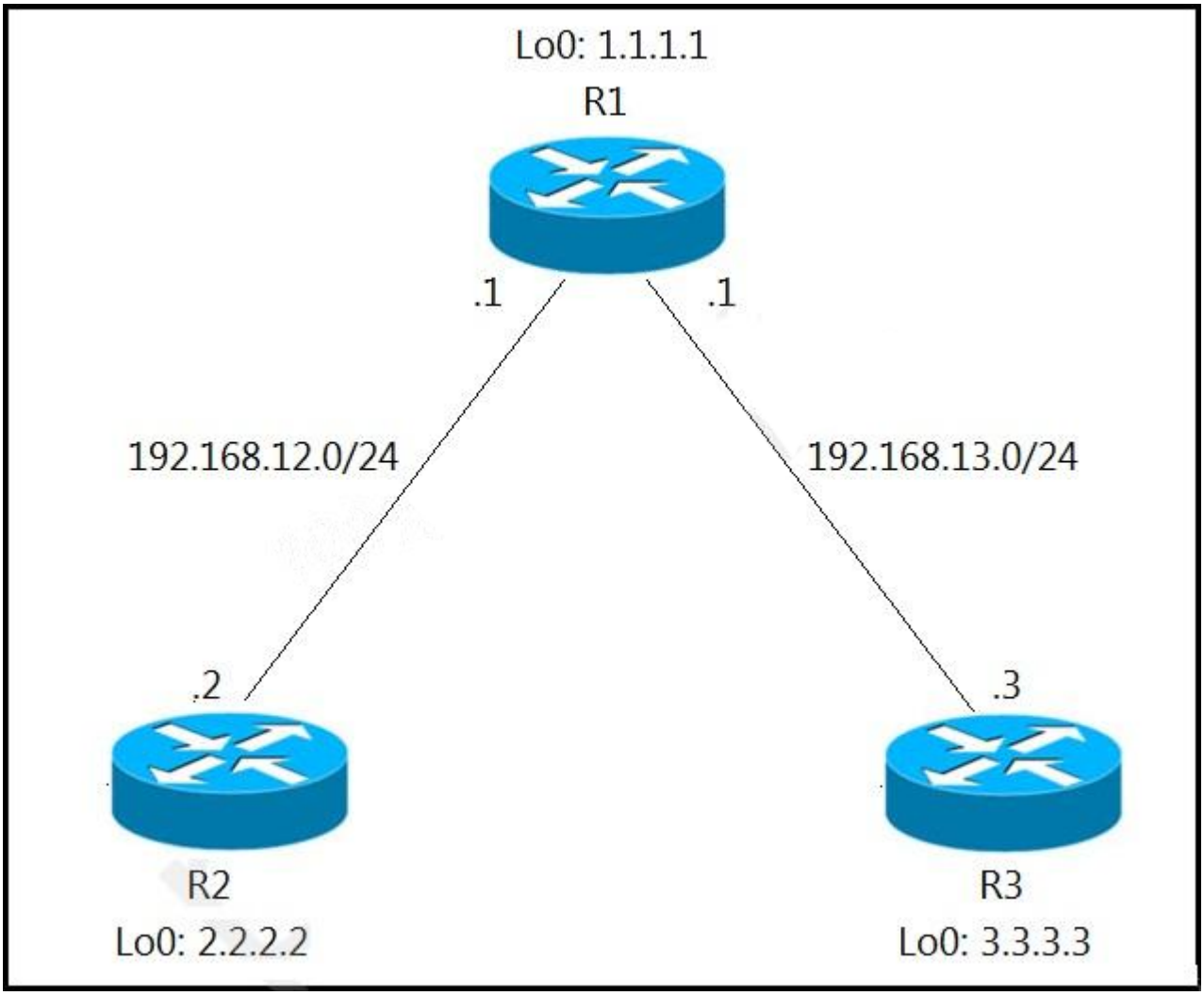
Answer: A

Explanation:

In this question, routes from EIGRP domain are redistributed into OSPF (with tag 111) then RIPv2 but without any filtering so R5 learns all routes from both EIGRP and OSPF domain. If we only want R5 to learn routes from OSPF domain then we must filter out routes with tag 111 and permit other routes.

The line “route-map O2R permit 20” is important to allow other routes because of the implicit deny all at the end of each route-map.

279.Refer to the exhibit.



An engineer has configured R1 as EIGRP stub router. After the configuration, router R3 failed to reach to R2 loopback address.

Which action advertises R2 loopback back into the R3 routing table?

A. Add a static route for R2 loopback address in R1 and redistribute it to advertise to R3.

B. Use a leak map on R1 that matches the required prefix and apply it with the distribute list command toward R3.

C. Use a leak map on R3 that matches the required prefix and apply it with the EIGRP stub feature.

D. Add a static null route for R2 loopback address in R1 and redistribute it to advertise to R3.

Answer: B
Explanation:
The EIGRP stub feature is useful to prevent unnecessary EIGRP queries and to filter some routes that you advertise.
What if you want to configure your router as a stub router but still make an exception to some routes that it advertises? That is possible with the leak-map feature.
This is how to configure leak-map in this question:
R1(config)#ip access-list standard R2_L0
R1(config-std-nacl)#permit host 2.2.2.2
R1(config)#route-map R2_L0_LEAK
R2(config-route-map)#match ip address R2_L0
R1(config)#router eigrp 1
R1(config-router)#eigrp stub leak-map R2_L0_LEAK

280.Refer to the exhibit.

```
R1#sh ip route
     10.0.0.0/8 is variably subnetted, 3 subnets, 1 masks
D       10.1.2.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
D       10.1.1.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
C       10.1.100.0/24 is directly connected, FastEthernet0/0
```

An engineer configures the router 10.1.100.10 for EIGRP autosummarization so that R1 should receive the summary route of 10.0.0.0/8. However, R1 receives more specific /24 routes.
Which action resolves this issue?
A. Router R1 should configure ip summary address eigrp (AS number) 10.0.0.0 255.0.0.0 for the R1 Fast Ethernet 0/0 connected interface.
B. Router R1 should configure ip route 10.0.0.0 255.0.0.0 null 0 for the routes that are received on R1.
C. Router 10.1.100.10 should configure ip route 10.0.0.0 255.0.0.0 null 0 for the routes that are summarized toward R1.
D. Router 10.1.100.10 should configure ip summary address eigrp (AS number) 10.0.0.0 255.0.0.0 for the R1 Fast Ethernet 0/0 connected interface.
Answer: D

281.DRAG DROP
Drag and drop the IPv6 first hop security device roles from the left onto the corresponding descriptions on the right.

host	Receives router advertisements from valid routers, and no router solicitation are received.
router	Receives router solicitation and sends router advertisements.
monitor	Receives valid and rogue router advertisements and all router solicitation.
switch	Received router advertisements are trusted and are flooded to synchronize states.

Answer:

host	router
router	host
monitor	switch
switch	monitor

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/security/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_7x_chapter_011011.pdf

282.Refer to the exhibit.

```
*17:40:07.826: AAA/BIND(00000055): Bind i/f
*17:40:07.826: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*17:40:07.826: TPLUS: Queuing AAA Authentication request 85 for processing
*17:40:07.826: TPLUS: TPLUS(00000055) login timer started 1020 sec timeout
*17:40:07.826: TPLUS: processing authentication start request id 85
*17:40:07.826: TPLUS: Authentication start packet created for 85()
*17:40:07.826: Using server 10.106.60.182
*17:40:07.826: TPLUS(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*17:40:07.830: TPLUS(00000055)/0/NB_WAIT: socket event 2
*17:40:07.830: TPLUS(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*17:40:07.830: TPLUS(00000055)/0/READ: socket event 1
*17:40:07.830: TPLUS(00000055)/0/READ: Would block while reading
*17:40:07.886: TPLUS(00000055)/0/READ: socket event 1
*17:40:07.886: TPLUS(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*17:40:07.886: TPLUS(00000055)/0/READ: socket event 1
*17:40:07.886: TPLUS(00000055)/0/READ: read entire 18 bytes response
*17:40:07.886: TPLUS(00000055)/0/225FE2DC: Processing the reply packet
*17:40:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*17:40:07.886: TPLUS: Invalid AUTHEN packet (check keys).
```

An engineer is troubleshooting a TACACS problem.
Which action resolves the issue?
A. Configure a matching TACACS server IP.
B. Configure a matching preshared key.
C. Generate authentication from a relative source interface.
D. Apply a configured AAA profile to the VTY.
Answer: B
Explanation:
Reference: https://community.cisco.com/t5/network-access-control/issues-with-tacacs-authentication/td-p/3412001
The last line shows us the reason, which is “Invalid AUTHEN packet (check keys)” so the most likely cause of this problem is key mismatch.

283.The network administrator configured CoPP so that all HTTP and HTTPS traffic from the administrator device located at 172.16 1.99 toward the router CPU is limited to 500 kbps. Any traffic that exceeds this limit must be dropped.
access-list 100 permit ip host 172.16.1.99 any
!
class-map CM-ADMIN

match access-group 100
!
policy-map PM-COPP
class CM-ADMIN
police 500000 conform-action transmit
!
interface E0/0
service-policy input PM-COPP
CoPP failed to capture the desired traffic and the CPU load is getting higher.
Which two configurations resolve the issue? (Choose two.)
A. interface E0/0
no service-policy input PM-COPP
!
control-plane
service-policy input PM-COPP
B. policy-map PM-COPP
class CM-ADMIN
no police 500000 conform-action transmit
police 500 conform-action transmit
!
control-plane
service-policy input PM-COPP
C. no access-list 100
access-list 100 permit tcp host 172.16.1.99 any eq 80
D. no access-list 100
access-list 100 permit tcp host 172.16.1.99 any eq 80
access-list 100 permit tcp host 172.16.1.99 any eq 443
E. policy-map PM-COPP
class CM-ADMIN
no police 500000 conform-action transmit
police 500 conform-action transmit
Answer: A

284.Refer to the exhibit.

```
ipv6 access-list INTERNET
 permit ipv6 2001:DB8:AD59:BA21::/64 2001:DB8:C0AB:BA14::/64
 permit tcp 2001:DB8:AD59:BA21::/64 2001:DB8:C0AB:BA13::/64 eq telnet
 permit tcp 2001:DB8:AD59:BA21::/64 any eq http
 permit ipv6 2001:DB8:AD59::/48 any
 deny ipv6 any any log
```

While monitoring VTY access to a router, an engineer notices that the router does not have any filter and anyone can access the router with username and password even though an ACL is configured.
Which command resolves this issue?
A. access-class INTERNET in
B. ip access-group INTERNET in

C. ipv6 traffic-filter INTERNET in
D. ipv6 access-class INTERNET in
Answer: D

285.Refer to the exhibit.

ipv6 dhcp server:

```
ipv6 unicast-routing
!
int e0/1
ipv6 enable
ipv6 add 2001:11::1/64
ipv6 nd other-config-flag
no shut
ipv6 dhcp server IPv6Pool
!
ipv6 dhcp pool IPv6Pool
dns-server 2002:555::1
domain-name my.net
```

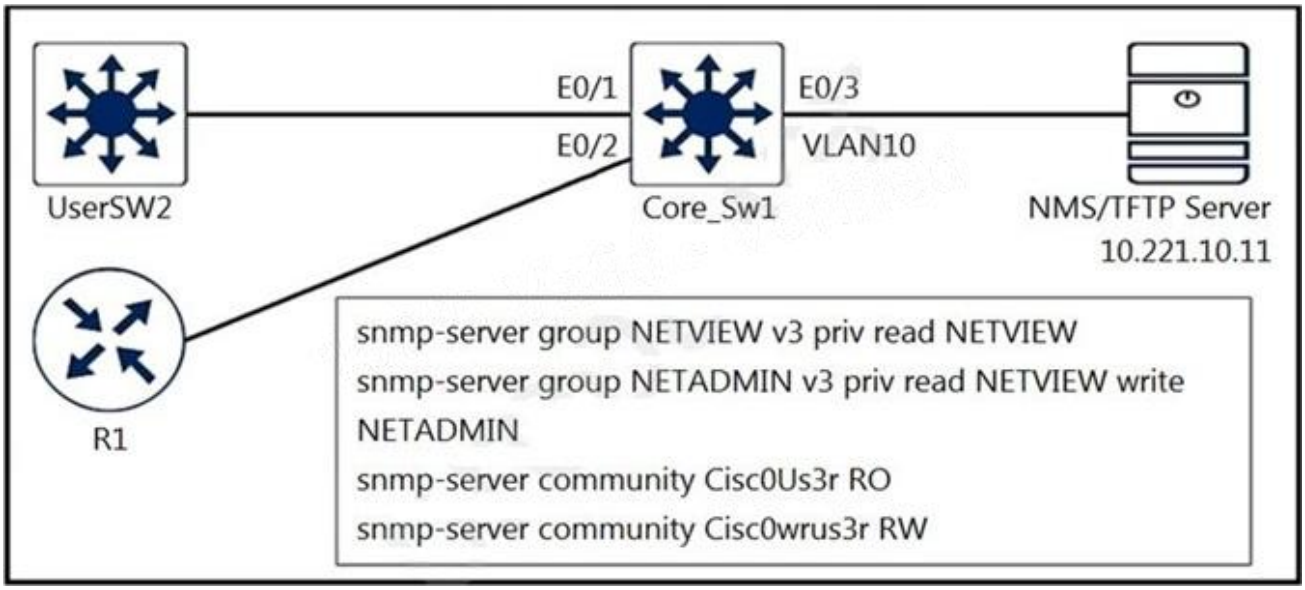
ipv6 dhcp client:

```
interface Ethernet0/1
no ip address
ipv6 address dhcp
ipv6 enable
no shut
```

A network administrator is troubleshooting IPv6 address assignment for a DHCP client that is not getting

an IPv6 address from the server.
Which configuration retrieves the client IPv6 address from the DHCP server?
A. ipv6 address autoconfig command on the interface
B. ipv6 dhcp server automatic command on DHCP server
C. ipv6 dhcp relay-agent command on the interface
D. service dhcp command on DHCP server
Answer: A

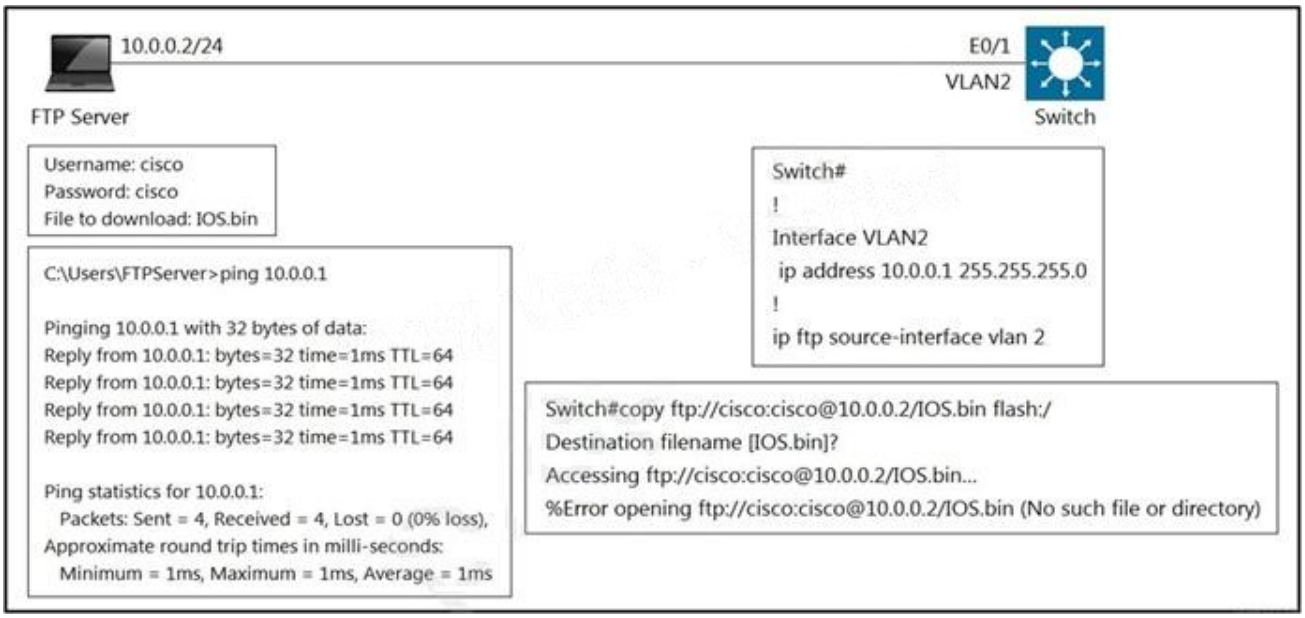
286.Refer to the exhibit.



A junior engineer configured SNMP to network devices. Malicious users have uploaded different configurations to the network devices using SNMP and TFTP servers.
Which configuration prevents changes from unauthorized NMS and TFTP servers?
A. access-list 20 permit 10.221.10.11
access-list 20 deny any log
!
snmp-server group NETVIEW v3 priv read NETVIEW access 20
snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 20
snmp-server community Cisc0Us3r RO 20
snmp-server community Cisc0wrus3r RW 20
snmp-server tftp-server-list 20
B. access-list 20 permit 10.221.10.11
access-list 20 deny any log
!
snmp-server group NETVIEW v3 priv read NETVIEW access 20
snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 20
snmp-server community Cisc0wrus3r RO 20
snmp-server community Cisc0Us3r RW 20
snmp-server tftp-server-list 20
C. access-list 20 permit 10.221.10.11
access-list 20 deny any log

D. access-list 20 permit 10.221.10.11
Answer: A

287.Refer to the exhibit.



An engineer cannot copy the IOS.bin file from the FTP server to the switch.
Which action resolves the issue?
A. Allow file permissions to download the file from the FTP server.
B. Add the IOS.bin file, which does not exist on FTP server.
C. Make memory space on the switch flash or USB drive to download the file.
D. Use the copy flash:/ ftp://cisco@10.0.0.2/IOS.bin command.
Answer: B

288.What does the MP-BGP OPEN message contain?
A. MPLS labels and the IP address of the router that receives the message
B. the version number and the AS number to which the router belongs
C. IP routing information and the AS number to which the router belongs
D. NLRI, path attributes, and IP addresses of the sending and receiving routers
Answer: B

289.Refer to the exhibit.

```
R1#sh ip route
     10.0.0.0/8 is variably subnetted, 3 subnets, 1 masks
D       10.1.2.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
D       10.1.1.0/24 [90/409600] via 10.1.100.10, 00:08:45,
FastEthernet0/0
C       10.1.100.0/24 is directly connected, FastEthernet0/0
```

Although summarization is configured for R1 to receive 10.0.0.0/8. more specific routes are received by R1.

How should the 10.0.0.0/8 summary route be received from the neighbor, attached to R1 via Fast Ethernet0/0 interface?
A. R1 should configure the ip summary-address eigrp <AS number> 10.0.0.0.255.0.0.0 command under the Fast Ethernet 0/0 interface.
B. The summarization condition is not met Router 10 1 100.10 requires a route for 10 0.0.0/8 that points to null 0
C. The summarization condition is not met. The network 10.1.100.0/24 should be changed to 172.16.0.0/24.
D. R1 should configure the ip summary-address eigrp <AS number> 10.0.0.0 0.0.0.255 command under the Fast Ethernet 0/0 interface.
Answer: D

290.Refer to the exhibit.

```
R1(config)#ip prefix-list EIGRP seq 10 deny 0.0.0.0/0 le 32
R1(config)#ip prefix-list EIGRP seq 20 permit 10.0.0.0/8
R1(config)#router eigrp 10
R1(config-router)#distribute-list prefix EIGRP in Ethernet0/0

R1#show ip route eigrp
```

A prefix list is created to filter routes inbound to an EIGRP process except for network 10 prefixes After the prefix list is applied no network 10 prefixes are visible in the routing table from EIGRP.
Which configuration resolves the issue?
A. ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9.
B. ip prefix-list EIGRP seq 10 permit 0.0.0.0/0 le 32
C. ip prefix-list EIGRP seq 5 permit 10.0.0.0/8 ge 9 no ip prefix-list EIGRP seq 20 permit 10.0.0.0/8
D. ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9 ip prefix-list EIGRP seq 10 permit 0.0.0.0/0 le 32
Answer: C

291.Refer to the exhibit.

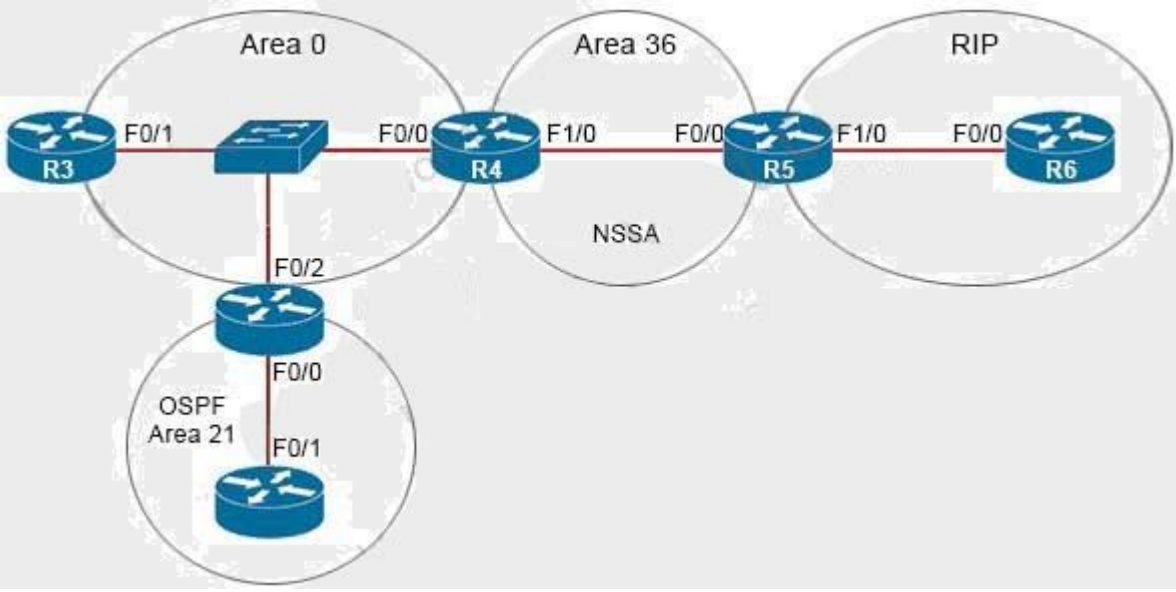
```
Tunnel source 199.1.1.1, destination 200.1.1.3
Tunnel protocol/transport GRE/IP
  Key disabled, sequencing disabled
  Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
Tunnel transport MTU 1476 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
```

An engineer must establish a point-to-point GRE VPN between R1 and the remote site.
Which configuration accomplishes the task for the remote site?
A. Interface Tunnel1
tunnel source 199.1.1.1
tunnel destination 200.1.1.3
ip address 192.168.1.3 255.255.255.0

B. Interface Tunnel1
tunnel source 200.1.1.3
tunnel destination 199.1.1.1
ip address 192.168.1.1.255.255.255.0
C. Interface Tunnel1
tunnel source 200.1.1.3
tunnel destination 199.1.1.1
ip address 192.168.1.3.255.255.255.0
D. Interface Tunnel
lunnel source 199.1.1.1
tunnel destination 200.1.1.3
ip address 192.168.1.1.255.255.255.0
Answer: C

292.What are the two prerequisites to enable BFD on Cisco routers? (Choose two)
A. A supported IP routing protocol must be configured on the participating routers.
B. OSPF Demand Circuit must run BFD on all participating routers.
C. ICMP must be allowed on all participating routers.
D. UDP port 1985 must be allowed on all participating routers.
E. Cisco Express Forwarding and IP Routing must be enabled on all participating routers.
Answer: C, E

293.Refer to the exhibit.



```
R5# show ip ospf 1 | begin Area 36
Area 36
Number of interfaces in this area is 2
It is a NSSA area
Area has no authentication
SPF algorithm last executed 00:32:46.376 ago
SFF algorithm executed 13 times
Area ranges are
172.16.0.0/16 Passive Advertise
```

The network engineer configured the summarization of the RIP routes into the OSPF domain on R5 but still sees four different 172.16.0.0/24 networks on R4.

Which action resolves the issue?

A. R5(config)#router ospf 1
R5(config-router)#no area
R5(config-router)#summary-address 172.16.0.0 255.255.252.0

B. R4(config)#router ospf 99
R4(config-router)#network 172.16.0.0 0.255.255.255 area 56
R4(config-router)#area 56 range 172.16.0.0 255,255.255.0

C. R4(config)#router ospf 1
R4(config-router)#no area
R4(config-router)#summary-address 172.16.0.0 255.255.252.0

D. R5(config)#router ospf 99
R5(config-router)#network 172.16.0.0 0.255.255.255 area 56
R5(config-router)#area 56 range 172.16.0.0 255.255.255.0

Answer: A

Explanation:

Area 36 is a NSSA so R5 is an ASBR so we can summarize external routes using the “summaryaddress” command. The command “areaarea-id range” can only be used on ABR so it is not correct.

The summarization must be done on the ASBR which is R5, not R4 so the correct answer must be started with “R5(config)#router ospf 1”.

Note: The “no area” command is used to remove any existing “area …” command (maybe “area 56 range …” command).

294.The network administrator configured the router for Control Plane Policing to limit OSPF traffic to be policed to 1 Mbps. Any traffic that exceeds this limit must also be allowed at this point for traffic analysis.

The router configuration is:

```
access-list 100 permit ospf any any
!
class-map CM-OSPF
match access-group 100
!
policy-map PM-COPP
class CM-OSPF
police 1000000 conform-action transmit
!
control-plane
```

service-policy output PM-COPP
The Control Plane Policing failed to monitor and police OSPF traffic.
Which configuration resolves this issue?
A. no access-list 100
access-list 100 permit tcp any any eq 179
access-list 100 permit ospf any any
access-list 101 permit tcp any any range 22 23
!
!
class-map CM-MGMT
 no match access-group 100
 match access-group 101
!
control-plane
 no service-policy output PM-COPP
 service-policy input PM-COPP
B. No access-list 100
access-list 100 permit tcp any any eq 179
access-list 100 permit tcp any any range eq 22
access-list 100 permit tcp any any range eq 23
access-list 100 permit ospf any any
C. control-plane
no service-policy output PM-COPP
service-policy input PM-COPP
D. no access-list 100
access-list 100 deny ospf any any
access-list 100 permit ip any any
!
policy-map PM-COPP
class CM-OSPF
no police 1000000 conform-action transmit
police 1000000 conform-action transmit
exceed-action drop
!
control-plane
no service-policy output PM-COPP
service-policy input PM-COPP
Answer: A

295.Which feature minimizes DoS attacks on an IPv6 network?
A. IPv6 Binding Security Table
B. IPv6 Router Advertisement Guard
C. IPv6 Prefix Guard
D. IPv6 Destination Guard

Answer: D
Explanation:
The Destination Guard feature helps in minimizing denial-of-service (DoS) attacks. It performs address resolutions only for those addresses that are active on the link, and requires the FHS binding table to be populated with the help of the IPv6 snooping feature. The feature enables the filtering of IPv6 traffic based on the destination address, and blocks the NDP resolution for destination addresses that are not found in the binding table. By default, the policy drops traffic coming for an unknown destination.
Reference:
https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book/IPv6_Security.pdf

296.Refer to Exhibit.

```
R1#sh ipv6 access-list GUARD
IPv6 access list GUARD
deny tcp any host 2001:DB8:A:B::10 eq telnet (6 matches) sequence 10
permit tcp host 2001:DB8:A:A::20 host 2001:DB8:A:B:10 eq telnet sequence 20
permit tcp host 2001:DB8:A:A::2 host 2001:DB8:D::1 eq www sequence 30
permit ipv6 2001:DB8:A:A::/64 any (67 matches) sequence 40
```

PC2 is directly connected to R1. A user at PC2 cannot Telnet to 2001:db8:a:b::10. The user can ping 2001:db8:a:b::10 and receive DHCP-related information from the DHCP server.
Which action resolves the issue?
A. Remove sequence 10 and put it back as sequence 25.
B. Remove sequence 20 and put it back as sequence 45.
C. Remove sequence 30 and put it back as sequence 5.
D. Remove sequence 40 and put it back as sequence 15.
Answer: A

297.A CoPP policy is applied for receiving SSH traffic from the WAN interface on a Cisco ISR4321 router.
However, the SSH response from the router is abnormal and stuck during the high link utilization. The problem is identified as SSH traffic does not match in the ACL.
Which action resolves the issue?
A. Rate-limit SSH traffic to ensure dedicated bandwidth.
B. Apply CoPP on the control plane interface.
C. Increase the IP precedence value of SSH traffic to 6.
D. Apply CoPP on the WAN interface inbound direction.
Answer: B
Explanation:
The problem is “SSH traffic does not match in the ACL” and “CoPP policy is applied for receiving SSH traffic from the WAN interface” so we should apply CoPP on the control plane interface instead.

298.Refer to the exhibit.

```
Router#show ip bgp vpnv4 rd 1100:1001 10.30.116.0/23
BGP routing table entry for 1100:1001:10.30.116.0/23, version 26765275
Paths: (9 available, best #6, no table)
 Advertised to update-groups:
   1    2      3
 (65001 64955 65003) 65089, (Received from a RR-dient)
       172.16.254.226 (metric 20645) from 172.16.224.236 (172.16.224.236)
        Origin IGP. metric 0, localpref 100, valid, confed-internal
        Extended Community: RT:1100:1001
        mpls labels in/out nolabel/362
 (65008 64955 65003) 65089
       172.16.254.226 (metric 20645) from 10.131.123.71 (10.131.123.71)
        Origin IGP, metric 0, localpref 100, valid, confed-external
        Extended Community: RT:1100:1001
        mpls labels in/out nolabel/362
 (65001 64955 65003) 65089
       172.16.254.226 (metric 20645) from 172.16.216.253 (172.16.216.253)
        Origin IGP, metric 0, localpref 100, valid, confed-external
        Extended Community: RT:1100:1001
        mpls labels in/out nolabel/362
 (65001 64955 65003) 65089
       172.16.254.226 (metric 20645) from 172.16.216.252 (172.16.216.252)
        Origin IGP, metric 0, localpref 100, valid, confed-external
        Extended Community: RT:1100:1001
        mpls labels in/out nolabel/362
 (64955 65003) 65089
       172.16.254.226   (metric 20645) from 10.77.255.57 (10.77.255.57)
        Origin IGP, metric 0, localpref 100, valid, confed-external
        Extended Community RT:1100:1001
        mpls labels in/out nolabel/362
 (64955 65003) 65089
       172.16.254.226 (metric 20645) from 10.57.255.11 (10.57.255.11)
        Origin IGP, metric 0, localpref 100, valid, confed-external, best
        Extended Community RT:1100:1001
        mpls labels in/out nolabel/362

 (64955 65003) 65089
  172.16.254.226 (metric 20645) from 172.16.224.253 (172.16.224.253)
  Origin IGP, metric 0, localpref 100, valid, confed-external
  Extended Community RT:1100:1001
  mpls labels in/out nolabel/362
 (65003) 65089
  172.16.254.226 (metric 20645) from 172.16.254.234 (172.16.254.234)
  Origin IGP, metric 0, localpref 100, valid, confed-external
       Extended Community RT:1100:1001
       mpls labels in/out nolabel/362
 65089, (Received from a RR-client)
  172.16.228.226 (metric 20645) from 172.16.228.226 (172.16.228.226)
  Origin IGP, metric 0, localpref 100, valid, confed-external
       Extended Community RT:1100:1001
       mpls labels in/out nolabel/278
```

An engineer configured BGP and wants to select the path from 10.77.255.57 as the best path instead of current best path.

Which action resolves the issue?
A. Configure AS_PATH prepend for the current best path
B. Configure higher MED to select as the best path
C. Configure AS_PATH prepend for the desired best path
D. Configure lower LOCAL_PREF to select as the best path
Answer: D
Explanation:
From the output, we learn that the current best path is from 10.57.255.11 (which includes "…valid, confed-external, best") and this path is 2 ASes away (64955 65003). Although there are some paths with only 1 AS away (path from 172.16.254.234 for example) but they were not chosen the best path so AS_PATH was not used to determine the best path -> Answers A and answer C are not correct.
All the paths in the output have metric of 0 and this is the lowest (best) value for this attribute. If we configure higher MED then it is less preferred over other paths -> Answer B is not correct.
Only answer D is left but LOCAL_PREF attribute should be configured with higher value to be preferred so we hope "lower LOCAL_PREF" here means higher value. But this is the best answer.

299.Refer to the exhibit.

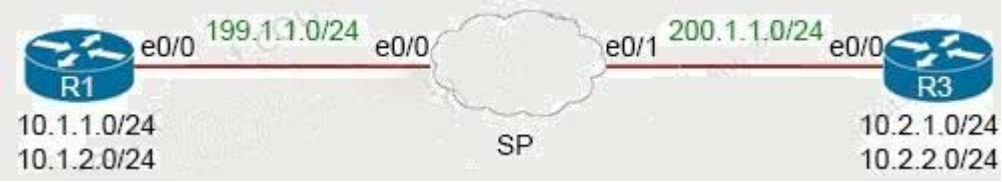
```
R2(config)# int tun0
*Jun 23 00:42:06.179: %LINEPR0T0-5-UPDOWN: Line protocol on
Interface Tunnel0, changed state to down

R2(config-if)# ip address 192.168.12.2 255.255.255.0
R2(config-if)# tunnel source lo0
R2(config-if)# tunnel destination 10.255.255.1

*Jun 23 00:42:15.845: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel0, changed state to up

R2(config-if)# router eigrp E
R2(config-router)# address-family ipv4 autonomous-system 1
R2(config-router-af)# net 192.168.12.2 0.0.0.0

*Jun 23 00:43:05.730: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor
192.168.12.1 (Tunnel0) is up: new adjacency
* Jun 23 00:43:05.993: %ADJ-5-PARENT: Midchain parent maintenance
for IP midchain out of Tunnel0 - looped chain attempting to stack
*Jun 23 00:43:15.193: %TUN-5-RECURD0WN: Tunnel0 temporarily
disabled due to recursive routing

*Jun 23 00:43:15.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel0, changed state to down
```

An administrator is configuring a GRE tunnel to establish an EIGRP neighbor to a remote router. The other tunnel endpoint is already configured. After applying the configuration as shown, the tunnel started flapping.
Which action resolves the issue?
A. Modify the network command to use the Tunnel0 interface netmask
B. Advertise the Loopback0 interface from R2 across the tunnel
C. Stop sending a route matching the tunnel destination across the tunnel

D. Readdress the IP network on the Tunnel0 on both routers using the /31 netmask
Answer: C
Explanation:
In this question we are advertising the tunnel IP address 192.168.12.2 to the other side. When other end receives the EIGRP advertisement, it realizes it can reach the other side of the tunnel via EIGRP.
In other words, it reaches the tunnel destination through the tunnel itself -> This causes “recursive routing” error.
Note: In order to avoid this error, do not advertise the tunnel destination IP address on the tunnel interface to other side.
Good recursive routing reference: https://networklessons.com/cisco/ccie-routing-switching/gretunnel-recursive-routing-error

300.Which two solutions are used to overcome a flapping link that causes a frequent label binding exchange between MPLS routers? (Choose two)
A. Create link dampening on links to protect the session.
B. Increase input queue on links to protect the session.
C. Create targeted hellos to protect the session.
D. Increase a hold-timer to protect the session.
E. Increase a session delay to protect the session.
Answer: A C
Explanation:
To avoid having to rebuild the LDP session altogether, you can protect it. When the LDP session between two directly connected LSRs is protected, a targeted LDP session is built between the two LSRs. When the directly connected link does go down between the two LSRs, the targeted LDP session is kept up as long as an alternative path exists between the two LSRs.
For the protection to work, you need to enable it on both the LSRs. If this is not possible, you can enable it on one LSR, and the other LSR can accept the targeted LDP Hellos by configuring the command mpls ldp discovery targeted-hello accept.
Reference: https://www.ccexpert.us/mpls-network/mpls-ldp-session-protection.html
Or from the reference at
https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/TECMPL-3201.pdf
Troubleshooting LDP Issues
Problem:
I. When a link flaps (for a short time),
…
Solution:
+ When LDP session supported by link hello is setup, create a targeted hello to protect the session.

301.Refer to the exhibit.



An engineer must configure a LAN-to-LAN IPsec VPN between R1 and the remote router.
Which IPsec Phase 1 configuration must the engineer use for the local router?
A. crypto isakmp policy 5
authentication pre-share
encryption 3des
hash sha
group 2
!
crypto isakmp key cisco123 address 200.1.1.3
B. crypto isakmp policy 5
authentication pre-share
encryption 3des
hash md5
group 2
!
crypto isakmp key cisco123 address 200.1.1.3
C. crypto isakmp policy 5
authentication pre-share
encryption 3des
hash md5
group 2
!
crypto isakmp key cisco123 address 199.1.1.1
D. crypto isakmp policy 5
authentication pre-share
encryption 3des
hash md5
group 2
!
crypto isakmp key cisco123! address 199.1.1.1
Answer: A
Explanation:
In the “crypto isakmp key … address” command, the address must be of the IP address of the other end (which is 200.1.1.3 in this case) so Option A and Option B are correct. The difference between these two options are in the hash SHA or MD5 method but both of them can be used although SHA is better than MD5 so we choose Option A the best answer.
Note: Cisco no longer recommends using 3DES, MD5 and DH groups 1, 2 and 5.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_imgmt/configuration/xe-16-5/sec-ipsec-management-xe-16-5-book/sec-ipsec-usability-enhance.html

302.What is a function of an end device configured with DHCPv6 guard?
A. If it is configured as a server, only prefix assignments are permitted.
B. If it is configured as a relay agent, only prefix assignments are permitted.
C. If it is configured as a client, messages are switched regardless of the assigned role.

D. If it is configured as a client, only DHCP requests are permitted.
Answer: C
Explanation:
The DHCPv6 Guard feature blocks reply and advertisement messages that come from unauthorized DHCP servers and relay agents.
Packets are classified into one of the three DHCP type messages. All client messages are always switched regardless of device role. DHCP server messages are only processed further if the device role is set to server. Further processing of server messages includes DHCP server advertisements (for source validation and server preference) and DHCP server replies (for permitted prefixes).
If the device is configured as a DHCP server, all the messages need to be switched, regardless of the device role configuration.

303.A customer requested a GRE tunnel through the provider network between two customer sites using loopback to hide internal networks.
Which configuration on R2 establishes the tunnel with R1?
A. R2(config)# interface Tunnel 1
R2(config-if)# ip address 172.20.1.2 255.255.255.0
R2(config-if)# ip mtu 1400
R2(config-if)# ip tcp adjust-mss 1360
R2(config-if)# tunnel source 192.168.20.1
R2(config-if)# tunnel destination 192.168.10.1
B. R2(config)# interface Tunnel 1
R2(config-if)# ip address 172.20.1.2 255.255.255.0
R2(config-if)# ip mtu 1400
R2(config-if)# ip tcp adjust-mss 1360
R2(config-if)# tunnel source 10.10.2.2
R2(config-if)# tunnel destination 10.10.1.1
C. R2(config)# interface Tunnel 1
R2(config-if)# ip address 172.20.1.2 255.255.255.0
R2(config-if)# ip mtu 1500
R2(config-if)# ip tcp adjust-mss 1360
R2(config-if)# tunnel source 192.168.20.1
R2(config-if)# tunnel destination 10.10.1.1
D. R2(config)# interface Tunnel 1
R2(config-if)# ip address 172.20.1.2 255.255.255.0
R2(config-if)# ip mtu 1500
R2(config-if)# ip tcp adjust-mss 1360
R2(config-if)# tunnel source 10.10.2.2
R2(config-if)# tunnel destination 10.10.1.1
Answer: D

304.A network administrator added a new spoke site with dynamic IP on the DMVPN network.
Which configuration command passes traffic on the DMVPN tunnel from the spoke router?
A. ip nhrp registration ignore

B. ip nhrp registration no-registration
C. ip nhrp registration dynamic
D. ip nhrp registration no-unique
Answer: D

305.Which IPv6 feature enables a device to reject traffic when it is originated from an address that is not stored in the device binding table?
A. IPv6 Snooping
B. IPv6 Source Guard
C. IPv6 DAD Proxy
D. IPv6 RA Guard
Answer: B
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-3s/ip6f-xe-3s-book/ip6-src-guard.html

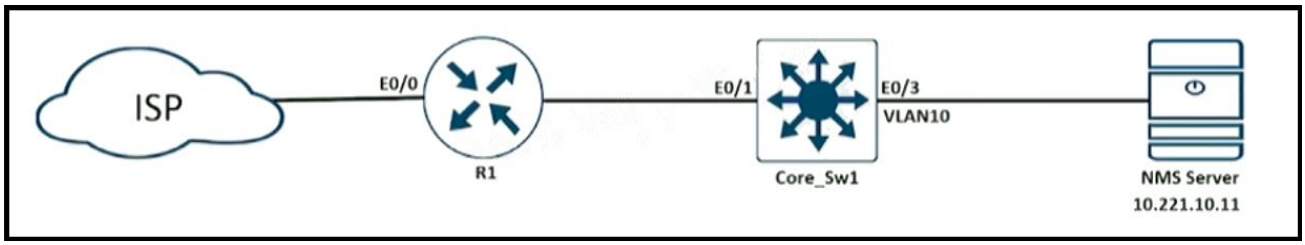
306.Refer to the exhibit.

```
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

D     10.0.0.0/8 [90/409600] via 172.16.1.200, 00:00:28, Ethernet0/0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.100/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback0
L        192.168.1.100/32 is directly connected, Loopback0
R1#
```

The R2 loopback interface is advertised with RIP and EIGRP using default values.
Which configuration changes make R1 reach the R2 loopback using RIP?
A. R1(config)# router rip
R1(config-router)# distance 90
B. R1(config)# router rip
R1(config-router)# distance 100
C. R1(config)# router eigrp 1
R1(config-router)# distance eigrp 130 120
D. R1(config)# router eigrp 1
R1(config-router)# distance eigrp 120 120

Answer: C
Explanation:
distance (AD Number u want to change to) (neighbor IP) (Wildcard Mask) (access-list number)

307.Refer to the exhibit.



During ISP router maintenance, the network produced many alerts because of the flapping interface.
Which configuration on R1 resolves the issue?
A. no snmp trap link-status
B. snmp trap link-status down
C. snmp trap ip verify drop-rate
D. ip verify drop-rate notify hold-down 60
Answer: D

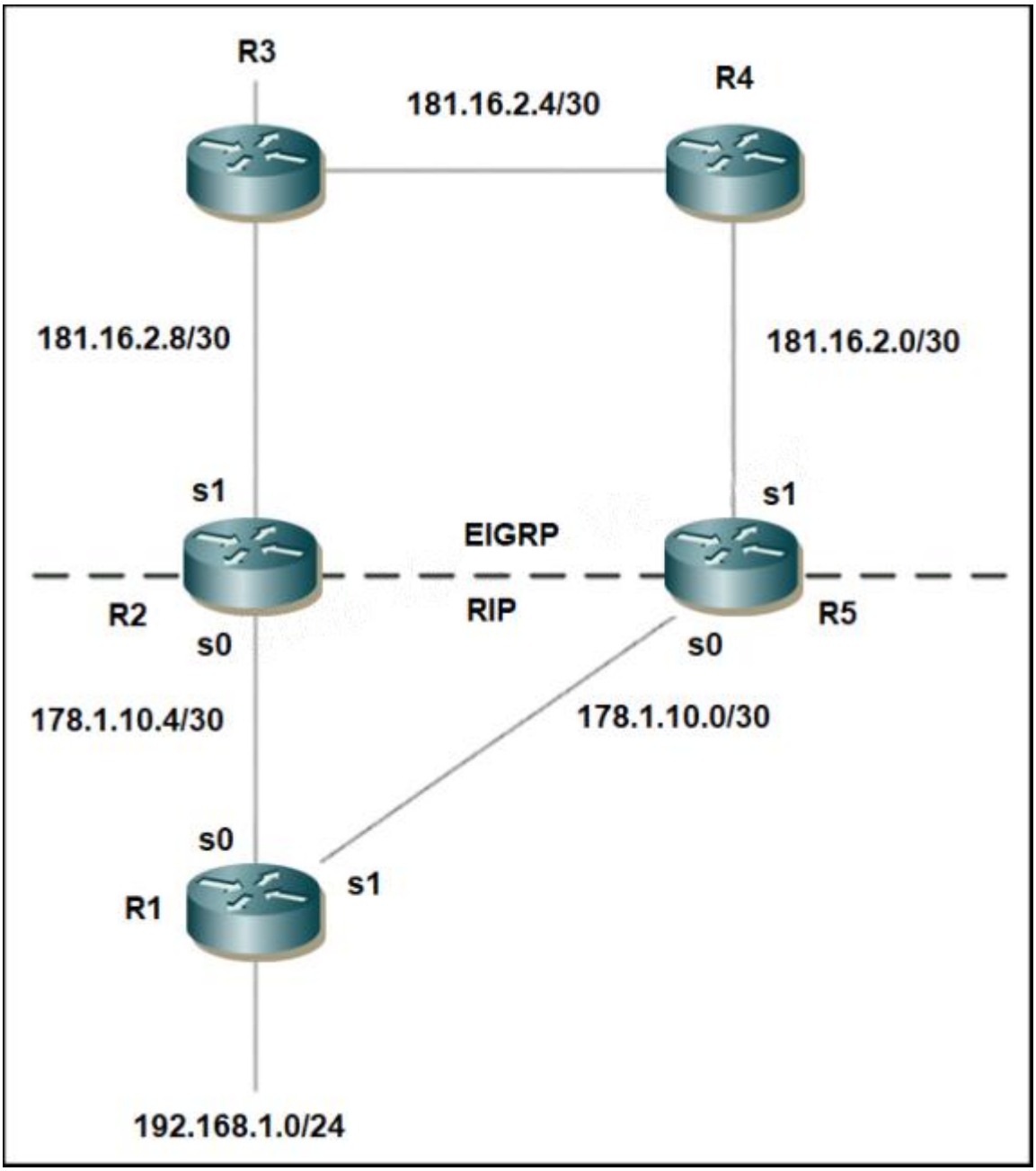
308.Refer to the exhibit.

```
ip vrf CCNP
 rd 1:1
interface Ethernet1
 ip vrf forwarding CCNP
 ip address 10.1.1.1 255.255.255.252
!
interface Ethernet2
 ip vrf forwarding CCNP
 ip address 10.2.2.2 255.255.255.252
```

Which configuration enables OSPF for area 0 interfaces to adjacency with a neighboring router with the same VRF?
A. router ospf 1 vrf CCNP
interface Ethernet1
ip ospf 1 area 0.0.0.0

interface Ethernet2
ip ospf 1 area 0.0.0.0
B. router ospf 1
interface Ethernet1
ip ospf 1 area 0.0.0.0
interface Ethernet2
ip ospf 1 area 0.0.0.0
C. router ospf 1 vrf CCNP
network 10.1.1.1 0.0.0.0 area 0
network 10.2.2.2 0.0.0.0 area 0
D. router ospf 1 vrf CCNP
network 10.0.0.0 0.0.255.255 area 0
Answer: C

309.Refer to the exhibit.



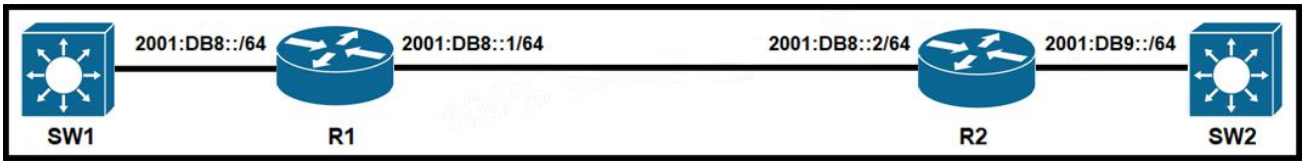
Mutual redistribution is enabled between RIP and EIGRP on R2 and R5.
Which configuration resolves the routing loop for the 192.168.1.0/24 network?
A. R2:
router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s1
!
router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!

access-list 1 deny 192.168.1.0
access-list 1 permit any
R5:
router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s0
!
router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
B. R2:
router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s0
!
router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
R5:
router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s0
!
router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
C. R2:
router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s0
!

router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
R5:
router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s1
!
router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
D. R2:
router eigrp 7
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s1
!
router rip
network 178.1.0.0
redistribute eigrp 7 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
R5:
router eigrp 7
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s1
!
router rip
network 178.1.0.0
redistribute eigrp 7 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
Answer: D
Explanation:

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.html

310.Refer to the exhibit.

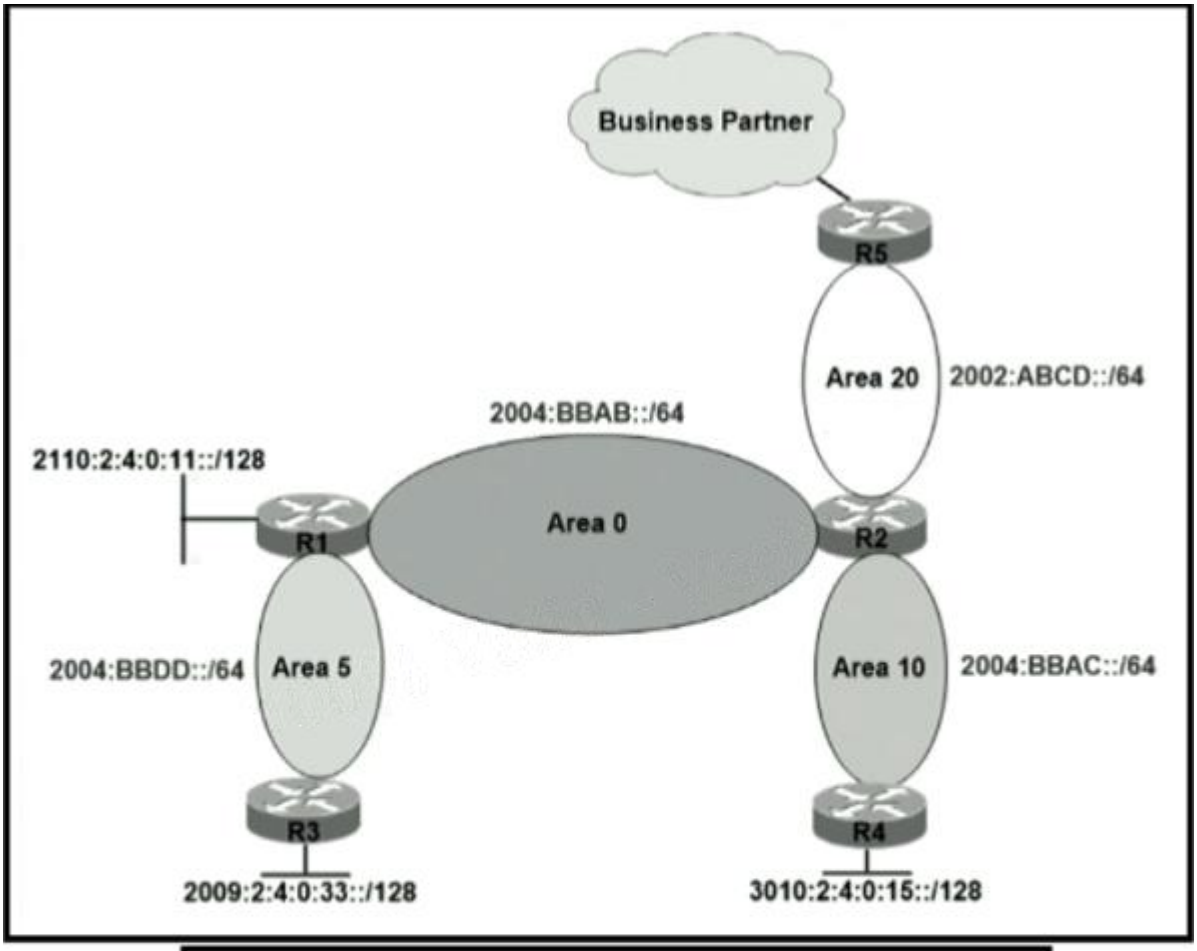


An engineer must advertise routes into IPv6 MP-BGP and failed.
Which configuration resolves the issue on R1?
A. router bgp 65000
no bgp default ipv4-unicast
address-family ipv6 multicast
network 2001:DB8::/64
B. router bgp 65000
no bgp default ipv4-unicast
address-family ipv6 unicast
network 2001:DB8::/64
C. router bgp 64900
no bgp default ipv4-unicast
address-family ipv6 unicast
network 2001:DB8::/64
D. router bgp 64900
no bgp default ipv4-unicast
address-family ipv6 multicast
neighbor 2001:DB8:7000::2 translate-update ipv6 multicast
Answer: B

311.An engineer failed to run diagnostic commands on devices using Cisco DNA Center.
Which action in Cisco DNA Center resolves the issue?
A. Enable Command Runner
B. Enable APIs
C. Enable CDP
D. Enable Secure Shell
Answer: A

312.Which two components are required for MPLS Layer 3 VPN configuration? (Choose two)
A. Use pseudowire for Layer 2 routes
B. Use MP-BGP for customer routes
C. Use OSPF between PE and CE
D. Use a unique RD per customer VRF
E. Use LDP for customer routes
Answer: CD

313.Refer to the exhibit.




```
R2#sh ipv6 route ospf
O   2002:ABCD::/64 [110/1]
     via FastEthernet0/1, directly connected
O   2004:BBAB::/64 [110/1]
     via FastEthernet0/0, directly connected
O   2004:BBAC::/64 [110/1]
     via FastEthernet1/0, directly connected
O   3010:2:4:0:15::/128 [110/1]
     via FE80::C804:1DFF:FE20:8, FastEthernet0/0
```

A network engineer applied a filter for LSA traffic on OSPFv3 interarea routes on the area 5 ABR to protect advertising the internal routes of area 5 to the business partner network. All other areas should receive the area 5 internal routes. After the respective route filtering configuration is applied on the ABR, area 5 routes are not visible on any of the areas.
How must the filter list be applied on the ABR to resolve this issue?
A. in the “in” direction for area 5 on router R1
B. in the “out” direction for area 5 on router R1
C. in the “in” direction for area 20 on router R2
D. in the “out” direction for area 20 on router R2
Answer: D

314.Refer to the exhibit.

```
ipv6 dhcp pool DHCPPOOL
address prefix 2001:0:1:4::/64 lifetime infinite infinite

interface FastEthernet0/0
ip address 10.0.0.1 255.255.255.240
duplex auto
speed auto
ipv6 address 2001:0:1:4::1/64
ipv6 enable
ipv6 nd ra suppress
ipv6 ospf 1 area 1
ipv6 dhcp server DHCPPOOL
```

Reachability between servers in a network deployed with DHCPv6 is unstable.
Which command must be removed from the configuration to make DHCPv6 function?
A. ipv6 dhcp server DHCPPOOL
B. ipv6 address 2001:0:1:4::/64
C. ipv6 nd ra suppress
D. address prefix 2001:0:1:4::/64 lifetime infinite infinite
Answer: C

315.Refer to the exhibit.

```
ip prefix-list DMZ-STATIC seq 5 permit 10.1.1.0/24
!
route-map DMZ permit 10
     match ip addresss prefix-list DMZ-STATIC
!
router ospf 1
network 0.0.0.0 0.0.0.0 area 0
redistribute static route-map DMZ
!
ip route 10.1.1.0 255.255.255.0 10.20.20.1
```

The static route is not present in the routing table of an adjacent OSPF neighbor router.
Which action resolves the issue?
A. Configure the next hop of 10.20.20.1 in the prefix list DMZ-STATIC

B. Configure the next-hop interface at the end of the static router for it to get redistributed
C. Configure a permit 20 statement to the route map to redistribute the static route
D. Configure the subnets keyword in the redistribution command
Answer: D

316.Refer to the exhibit.

```
!-- ACL for CoPP Routing class-map
!
access-list 120 permit tcp any gt 1024 eq bgp log
access-list 120 permit tcp any bgp gt 1024 established
access-list 120 permit tcp any gt 1024 eq 639
access-list 120 permit tcp any eq 639 gt 1024 established
access-list 120 permit tcp any eq 646
access-list 120 permit udp any eq 646
access-list 120 permit ospf any
access-list 120 permit ospf any host 224.0.0.5
access-list 120 permit ospf any host 224.0.0.6
access-list 120 permit eigrp any
access-list 120 permit eigrp any host 224.0.0.10
access-list 120 permit udp any any eq pim-auto-rp
```

The control plane is heavily impacted after the CoPP configuration is applied to the router.
Which command removal lessens the impact on the control plane?
A. access-list 120 permit udp any any eq pim-auto-rp
B. access-list 120 permit eigrp any host 224.0.0.10
C. access-list 120 permit ospf any
D. access-list 120 permit tcp any gt 1024 eq bgp log
Answer: A

317.Refer to the exhibit.

```
snmp-server community Public RO 90
snmp-server community Private RW 90
R1#show access-list 90
Standard IP access list 90
    permit 10.11.110.11
    permit 10.11.111.12

Nov 6 06:45:11: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host
10.11.110.12
Nov 6 06:45:12: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req from host
10.11.110.12
```

A network administrator notices these console messages from host 10.11.110.12 originating from interface E1/0. The administrator considers this an unauthorized attempt to access SNMP on R1.
Which action prevents the attempts to reach R1 E1/0?

A. Configure IOS control plane protection using ACL 90 on interface E1/0
B. Configure IOS management plane protection using ACL 90 on interface E1/0
C. Create an inbound ACL on interface E1/0 to deny SNMP from host 10.11.110.12
D. Add a permit statement including the host 10.11.110.12 into ACL 90

Answer: C

318.Refer to the exhibit.

```
CPE# ping 10.0.2.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.2.4, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/1/1 ms
CPE# copy flash:/packages.conf tftp://10.0.2.4/
Address or name of remote host [10.0.2.4]?
Destination filename [packages.conf]?
%Error opening tftp://10.0.2.4/packages.conf (Undefined error)
```

The administrator is trying to overwrite an existing file on the TFTP server that was previously uploaded by another router. However, the attempt to update the file fails.
Which action resolves this issue?

A. Make the packages.conf file executable by all on the TFTP server
B. Make the packages.conf file writable by all on the TFTP server
C. Make sure to run the TFTP service on the TFTP server
D. Make the TFTP folder writable by all on the TFTP server

Answer: B

319.Refer to the exhibit.

```
R2#show ip route

Gateway of last resort is not set
   10.0.0.0/8 is variably subnetted, 12 subnets, 3 masks
C     10.1.3.0/30 is directly connected, FastEthernet0/1
C     10.1.2.0/30 is directly connected, FastEthernet0/0
C     10.1.1.0/30 is directly connected, FastEthernet1/0
O E2  10.19.0.0/24 [110/20] via 10.1.3.2, 00:02:04, FastEthernet0/1
D     10.55.13.0/24 (90/4096001 via 10.1.2.2. 00:01:00. FastEthernet0/0
D     10.37.100. 0/24 (90/4096001 via 10.1.2.2. 00:01:00. FastEthernet0/0
C     10.100.10.0/29 is directly connected, FastEthernet2/0.10
D     10.55.72.0/24 (90/409600] via 10.1.2.2. 00:01:01. FastEthernet0/0
C     10.100.20.0/29 is directly connected. FastEthernet2/0.20
O E2  10.144.1.0/24 /110/201 via 10.1.3.2. 00:12:51. FastEthernet0/1
D     10.55.144.0/24 (90/4096001 via 10.1.2.2. 00:01:01. FastEthernet0/0
O E2  10.123.187.0/24 (110/20] via 10.1.3.2. 00:12:51, FastEthernet0/1
```

```
R2#sh ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(10.100.20.2)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r- reply Status, s - sia Status
P 10.1.3.0/30, 1 successors, FD is 281600 via Connected, FastEthernet0/1
P 10.1.2.0/30, 1 successors, FD is 281600 via Connected, FastEthernet0/0
P 10.1.1.0/30, 1 successors, FD is 28160 via Connected, FastEthernet1/0
P 10.55.13.0/24, 1 successors, FD is 409600 via 10.1.2.2 (409600/128256). FastEthernet0/0
P 10.37.100.0/24, 1 successors, FD is 409600 via 10.1.2.2 (409600/128256). FastEthernet0/0
P 10.55.72.0/24. 1 successors. FD is 409600 via 10.1.2.2 (409600/128256), FastEthernet0/0
P 10.55.144.0/24. 1 successors, FD is 409600 via 10.1.2.2 (409600/128256), FastEthernet0/0
P 10.123.187.0/24. 0 successors, FD is Inaccessible via 10.1.2.2 (409600/128256), FastEthernet0/0
```

Router R2 should be learning the route for 10.123.187.0/24 via EIGRP.

Which action resolves the issue without introducing more issues?

A. Use distribute-list to modify the route as an internal EIGRP route

B. Redistribute the route in EIGRP with metric, delay, and reliability

C. Use distribute-list to filter the external router in OSPF

D. Remove route redistribution in R2 for this route in OSPF

Answer: C

320.Refer to the exhibit.

```
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   192.168.10.1            Se1/0            12 00:00:39    1  5000  2  0
*Jan  1 15:40:21.295: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.10.1 (Serial1/0) is down: retry limit exceeded
*Jan  1 15:40:51.567: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.10.1 (Serial1/0) is up: new adjacency
*Jan  1 15:42:11.107: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.10.1 (Serial1/0) is down: retry limit exceeded
*Jan  1 15:42:14.879: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.10.1 (Serial1/0) is up: new adjacency


R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
```

R1 Configuration:

```
key chain cisco
key 2
  key-string abc
!
interface Loopback0
ip address 10.10.1.1 255.255.255.0
!
interface Serial1/0
ip address 192.168.10.1 255.255.255.0
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 cisco
serial restart-delay 0
!
router eigrp 100
network 10.10.1.0 0.0.0.255
network 192.168.10.0
no auto-summary
```

R2 configuration:

```
key chain cisco
key 1
  key-string 123
key 2
  key-string abc
!
interface Loopback0
ip address 10.10.2.2 255.255.255.0
!
interface Serial1/0
ip address 192.168.10.2 255.255.255.0
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 cisco
no fair-queue
!
!
router eigrp 100
network 10.10.2.0 0.0.0.255
network 192.168.10.0
no auto-summary
```

R1 and R2 are configured for EIGRP peering using authentication and the neighbors failed to come up. Which action resolves the issue?

A. Configure a matching key-id number on both routers

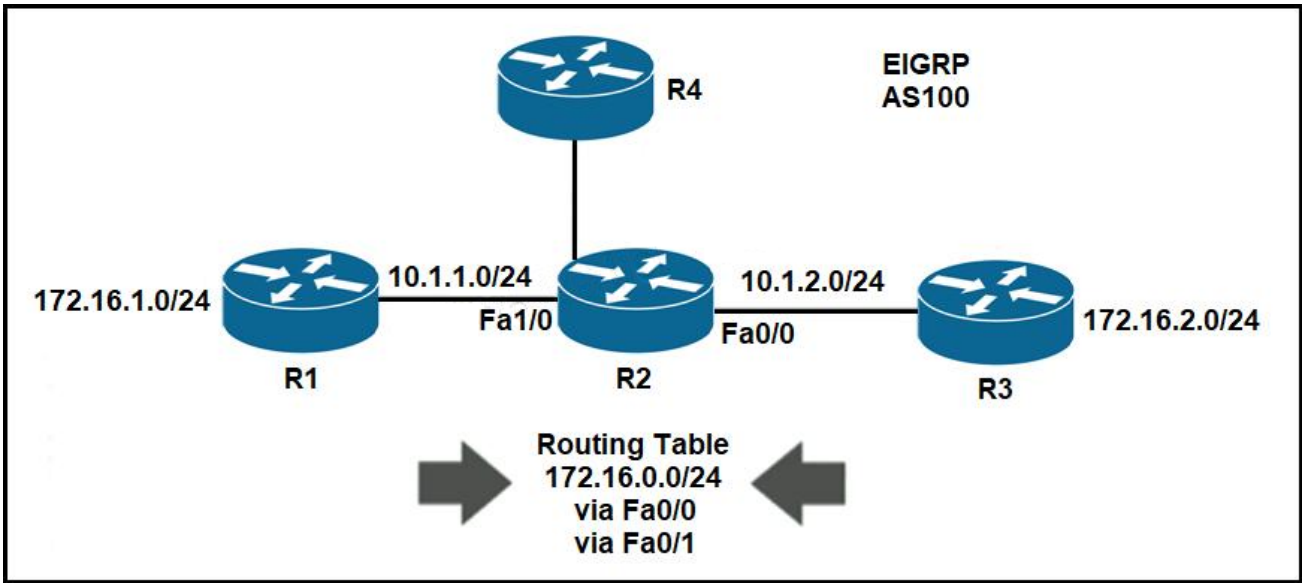
B. Configure a matching lowest key-id on both routers

C. Configure a matching key-chain name on both routers

D. Configure a matching authentication type on both router

Answer: A

321.Refer to the exhibit.



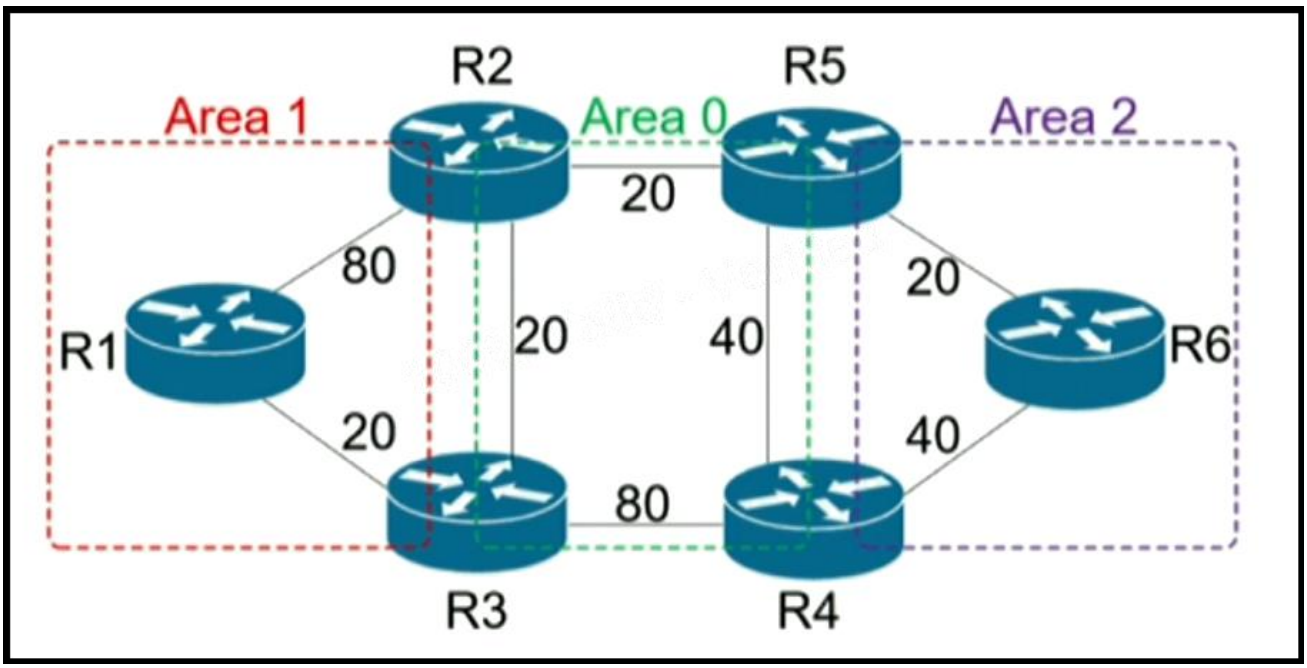
R4 is experiencing packet drop when trying to reach 172.16.2.7 behind R2.
Which action resolves the issue?
A. Insert a /16 floating static route on R2 toward R3 with metric 254
B. Insert a /24 floating static route on R2 toward R3 with metric 254
C. Enable auto summarization on all three routers R1, R2, and R3
D. Disable auto summarization on R2
Answer: D

322.Refer to the exhibit.

```
access-list 1 permit 209.165.200.215
access-list 2 permit 209.165.200.216
!
interface ethernet 1
ip policy route-map Texas
!
route-map Texas permit 10
match ip address 1
set ip precedence priority
set ip next-hop 209.165.200.217
!
route-map Texas permit 20
match ip address 2
set ip next-hop 209.165.200.218
```

Packets arriving from source 209.165.200.215 must be sent with the precedence bit set to 1, and packets arriving from source 209.165.200.216 must be sent with the precedence bit set to 5.
Which action resolves the issue?
A. set ip precedence critical in route-map Texas permit 10
B. set ip precedence critical in route-map Texas permit 20
C. set ip precedence immediate in route-map Texas permit 10
D. set ip precedence priority in route-map Texas permit 20
Answer: B

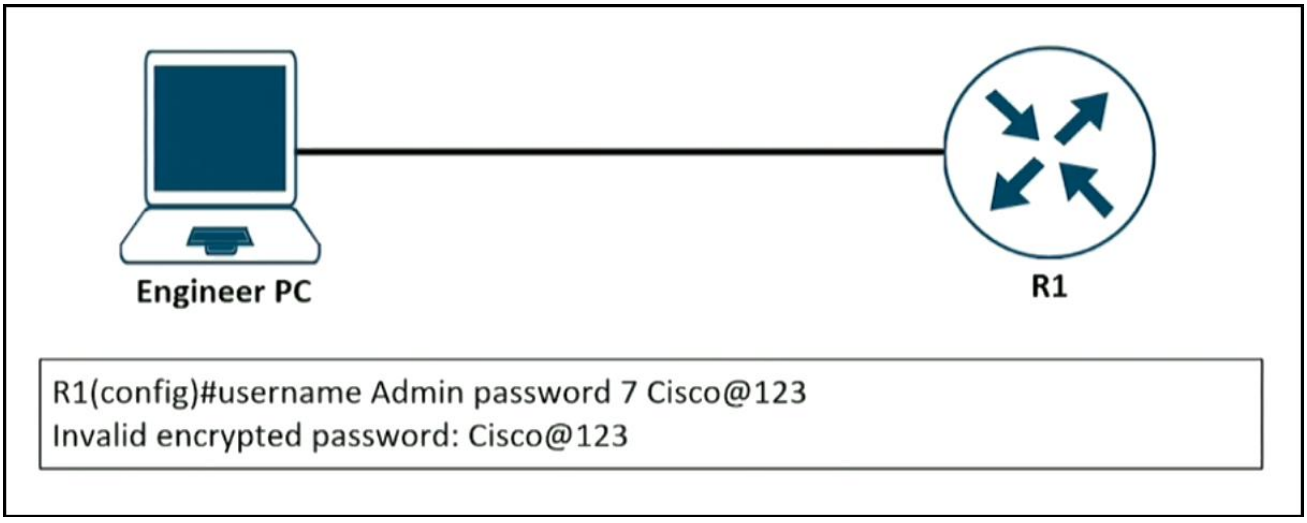
323.Refer to the exhibit.



R6 should reach R1 via R5>R2>R1.
Which action resolves the issue?
A. Increase the cost to 61 between R2-R3-R1
B. Increase the cost to 61 between R2 and R3
C. Decrease the cost to 2 between R6-R5-R2
D. Decrease the cost to 41 between R2 and R1
Answer: B

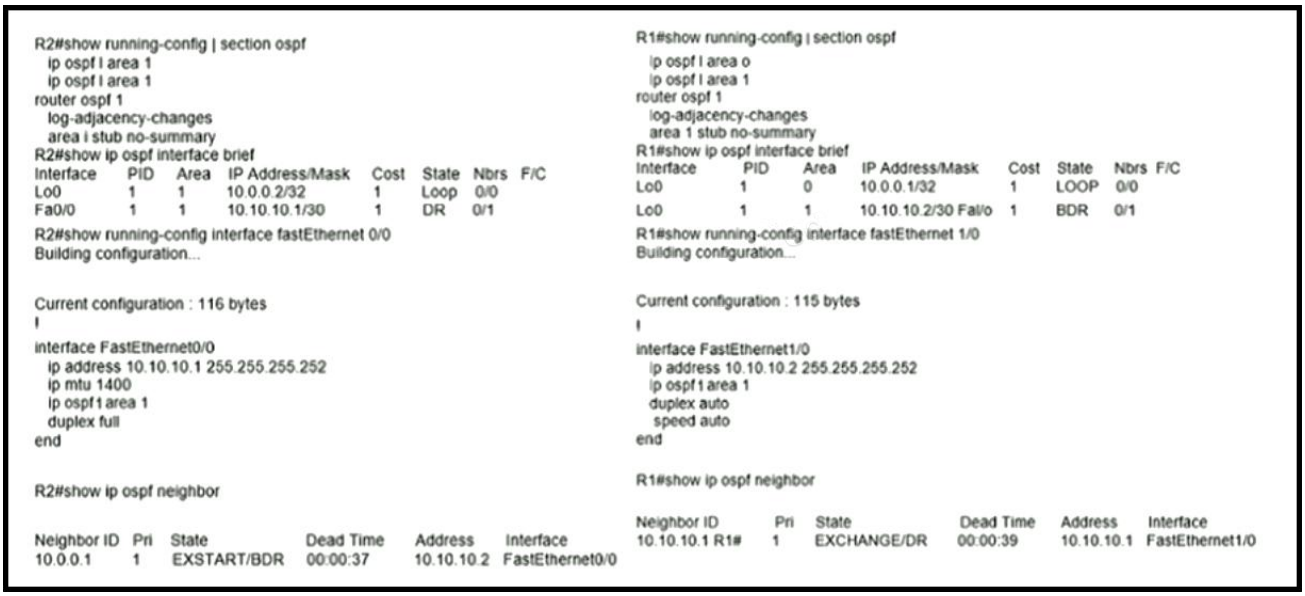
324.Which method provides failure detection in BFD?
A. short duration, high overhead
B. short duration, low overhead
C. long duration, high overhead
D. long duration, low overhead
Answer: B

325.Refer to the exhibit.



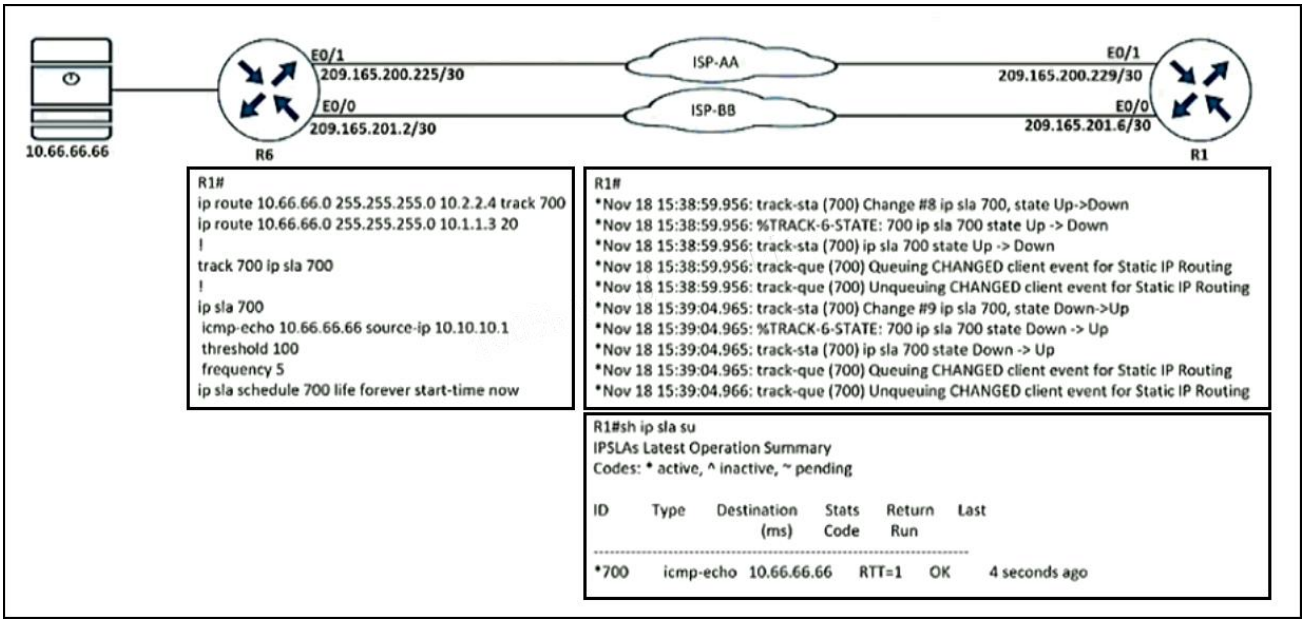
An engineer is trying to add an encrypted user password that should not be visible in the router configuration.
Which two configuration commands resolve the issue? (Choose two)
A. password encryption aes
B. username Admin password Cisco@maedeh motamedi
C. username Admin password 5 Cisco@maedeh motamedi
D. username Admin secret Cisco@maedeh motamedi
E. no service password-encryption
F. service password-encryption
Answer: DF

326.Refer to the exhibit.



Which action restores OSPF adjacency between R1 and R2?
A. Change the IP MTU of R1 Fa1/0 to 1300
B. Change the IP MTU of R2 Fa0/0 to 1300
C. Change the IP MTU of R1 Fa1/0 to 1500
D. Change the IP MTU of R2 Fa0/0 to 1500
Answer: D

327.Refer to the exhibit.



R1 is configured with IP SLA to check the availability of the server behind R6 but it kept failing.
Which configuration resolves the issue?

A. R1(config)# ip sla 700
R1(config-track)# delay down 30 up 20

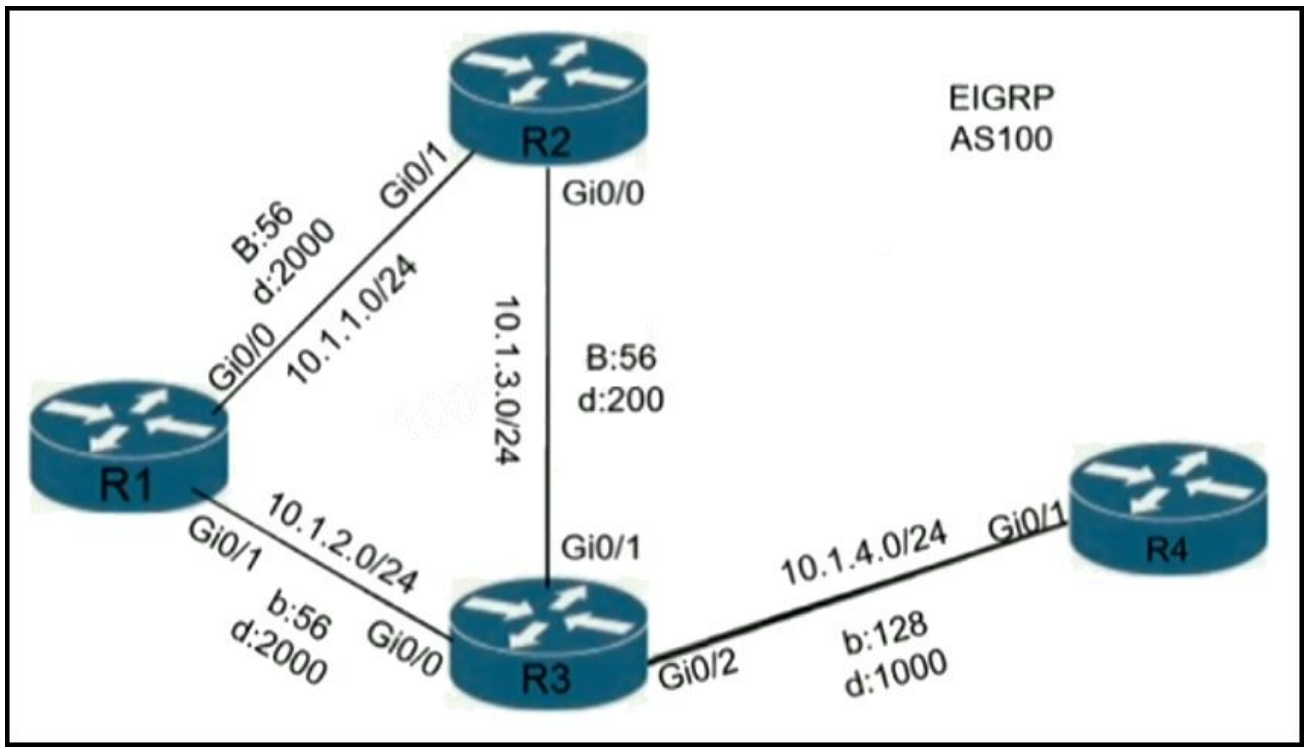
B. R1(config)# ip sla 700
R1(config-track)# delay down 20 up 30

C. R1(config)# track 700 ip sla 700
R1(config-track)# delay down 30 up 20

D. R1(config)# track 700 ip sla 700
R1(config-track)# delay down 20 up 30

Answer: C

328.Refer to the exhibit.



A loop occurs between R1, R2, and R3 while EIGRP is run with poison reverse enabled.
Which action prevents the loop between R1, R2, and R3?
A. Configure route tagging
B. Enable split horizon
C. Configure R2 as stub receive-only
D. Configure route filtering
Answer: C

329.A customer reports that traffic is not passing on an EIGRP enabled multipoint interface on a router configured as below:
interface Serial0/0
no ip address
interface Server0/0/0.9 multipoint
ip address 10.1.1.1 255.255.255.248
ip split-horizon eigrp 1
Which action resolves the issue?
A. Enable poison reverse
B. Enable split horizon
C. Disable poison reverse
D. Disable split horizon
Answer: D

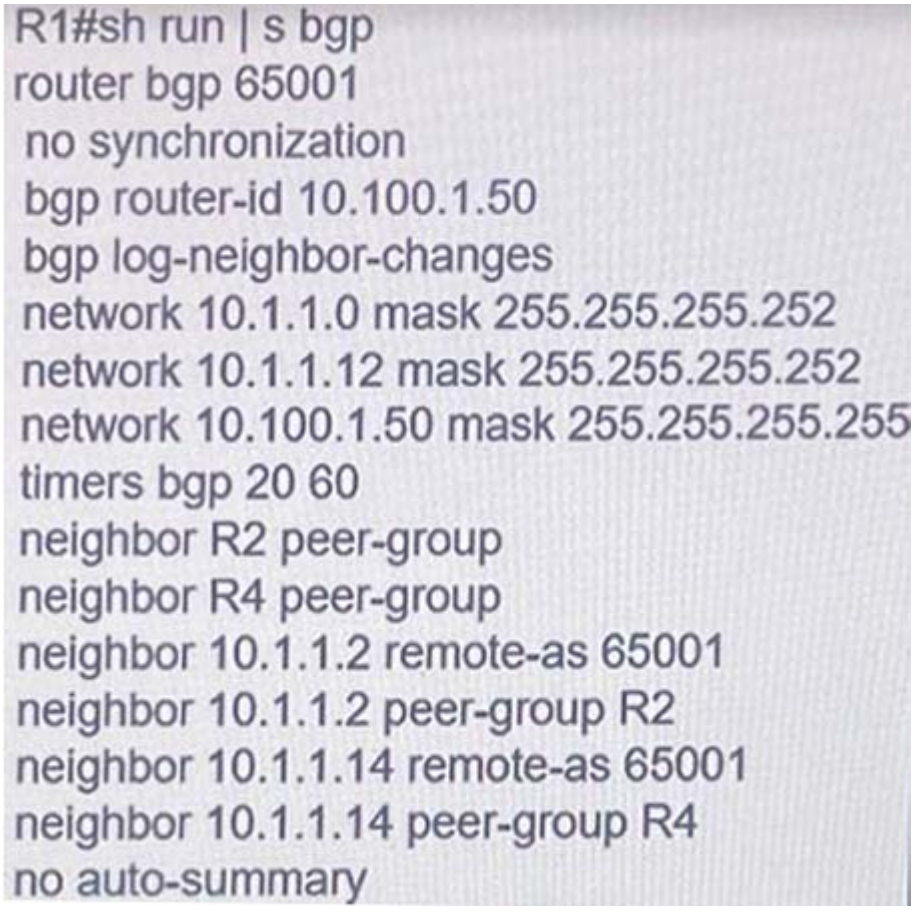
330.A newly installed spoke router is configured for DMVPN with the ip mtu 1400 command.
Which configuration allows the spoke to use fragmentation with the maximum negotiated TCP MTU over GRE?
A. ip tcp adjust-mss 1360

crypto ipsec fragmentation after-encryption
B. ip tcp adjust-mtu 1360
crypto ipsec fragmentation after-encryption
C. ip tcp adjust-mss 1360
crypto ipsec fragmentation mtu-discovery
D. ip tcp adjust-mtu 1360
crypto ipsec fragmentation mtu-discovery
Answer: A
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html

331.What are the two goals of micro BFD sessions? (Choose two.)
A. The high bandwidth member link of a link aggregation group must run BFD
B. Run the BFD session with 3x3 ms hello timer
C. Continuity for each member link of a link aggregation group must be verified
D. Eny member link on a link aggregation group must run BFD
E. Each member link of a link aggregation group must run BFD.
Answer: CE
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/xe-16-8/irb-xe-16-8-book/irb-micro-bfd.html

332.An engineer configured a router with this configuration
ip access-hst DENY TELNET
10 deny tcp any any eq 23 log-input
The router console starts receiving log message:
%SEC-6-IPACCESSLOGP: list DENY_TELNET denied tcp 192.168.1.10(1022) (FastEthernet1/0 D508.89gb.003f) ->192.168.2.20(23), 1 packet"
Which action stops messages on the console while still denying Telnet?
A. Configure a 20 permit ip any any command
B. Remove log-Input keyword from the access list.
C. Replace log-input keyword with the log keyword in the access list.
D. Configure a 20 permit ip any any log-input command.
Answer: B

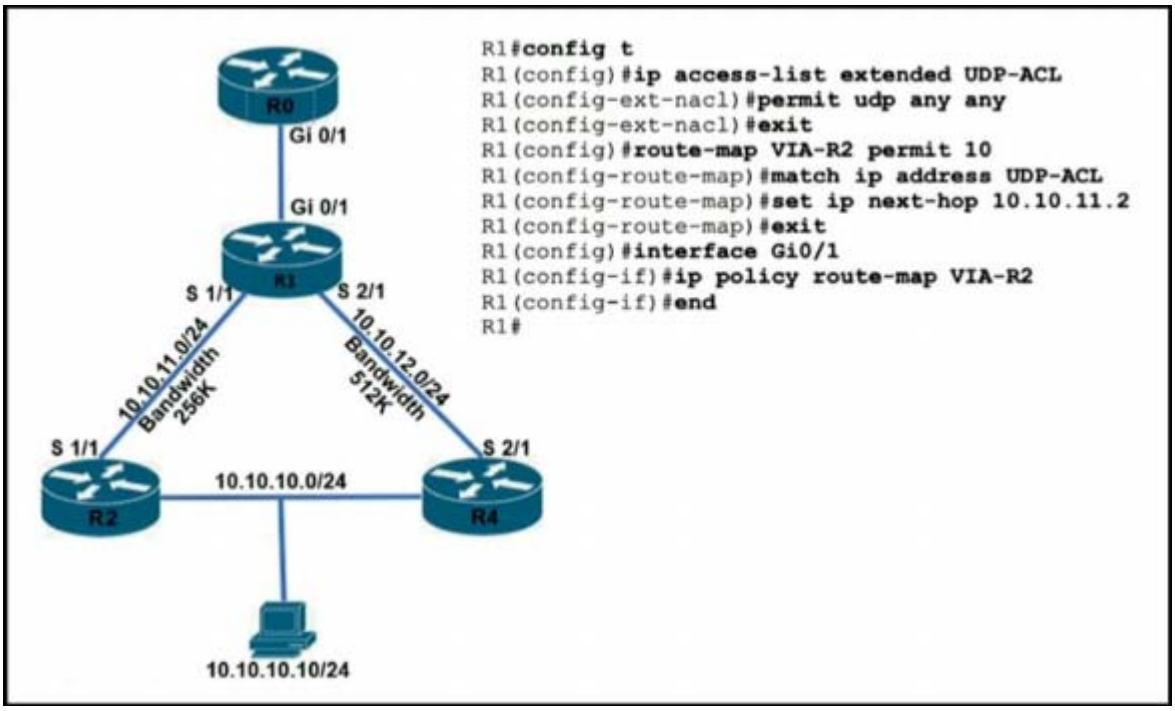
333.Refer to the exhibit.



While troubleshooting a BGP route reflector configuration, an engineer notices that reflected routes are missing from neighboring routers.
Which two BGP configurations are needed to resolve the issue? (Choose two)
A. neighbor 10.1.1.14 route-reflector-client
B. neighbor R2 route-reflector-client
C. neighbor 10.1.1.2 allowas-in
D. neighbor R4 route-reflector-client
E. neighbor 10.1.1.2 route-reflector-client
Answer: AE

334.Which IPv6 first hop security feature controls the traffic necessary for proper discovery of neighbor device operation and performance?
A. RA Throttling
B. Source or Destination Guard
C. ND Multicast Suppression
D. IPv6 Snooping
Answer: D

335.Refer to the exhibit.



TCP traffic should be reaching host 10.10.10.10/24 via R2.
Which action resolves the issue?
A. TCP traffic will reach the destination via R2 without any changes
B. Add a permit 20 statement in the route map to allow TCP traffic
C. Allow TCP in the access list with no changes to the route map
D. Set IP next-hop to 10. 10.12.2 under the route-map permit 10 to allow TCP traffic.
Answer: C

336.A network administrator must optimize the segment size of the TCP packet on the DMVPN IPsec protected tunnel interface, which carries application traffic from the head office to a designated branch. The TCP segment size must not overwhelm the MTU of the outbound link.
Which configuration must be applied to the router to improve the application performance?

```
interface tunnel30
 ip mtu 1400
 ip tcp packet-size 1360
!
crypto ipsec fragmentation after-encryption
```

```
interface tunnel30
 ip mtu 1400
 ip tcp payload-size 1360
!
crypto ipsec fragmentation before-encryption
```

```
interface tunnel30
 ip mtu 1400
 ip tcp adjust-mss 1360
!
crypto ipsec fragmentation after-encryption
```

```
interface tunnel30
 ip mtu 1400
 ip tcp max-segment 1360
!
crypto ipsec fragmentation before-encryption
```

A. Option A

B. Option B
C. Option C
D. Option D
Answer: C

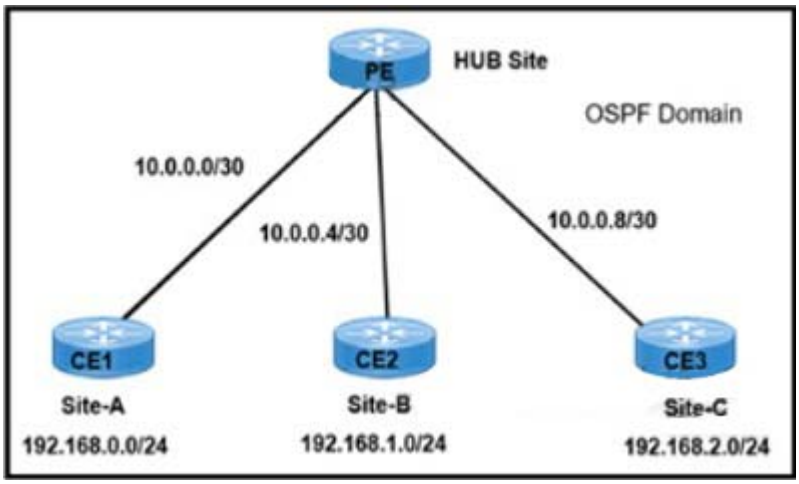
337.Refer to the exhibit.

```
R1# show ip ospf database self-originate

            OSPF Router with ID (10.255.255.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
Link count
10.255.255.1    10.255.255.1    4           0x800003BD 0x001AD9
3

                Summary Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.0.34.0       10.255.255.1    3604        0x80000380 0x00276C
10.255.255.4    10.255.255.1    3604        0x80000380 0x00762B

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum
Tag
0.0.0.0         10.255.255.1    3604        0x800001D0 0x001CBC
0



*Feb 22 22:50:39.523: %OSPF-4-FLOOD_WAR: Process 1 flushes LSA
ID 0.0.0.0 type-5 adv-rtr 10.255.255.1 in area 0
```

After configuring OSPF in R1, some external destinations in the network became unreachable.
Which action resolves the issue?
A. Clear the OSPF process on R1 to flush stale LSAs sent by other routers.
B. Change the R1 router ID from 10.255.255.1 to a unique value and clear the process.
C. Increase the SPF delay interval on R1 to synchronize routes.
D. Disconnect the router with the OSPF router ID 0.0.0.0 from the network.
Answer: B

338.What is the function of BFD?
A. It provides uniform failure detection regardless of media type.
B. It creates high CPU utilization on hardware deployments.
C. It negotiates to the highest version if the neighbor version differs.
D. It provides uniform failure detection on the same media type.
Answer: A

339.Refer to the exhibit.



A network engineer must establish communication between three different customer sites with these requirements:

- Site-A: must be restricted to access to any users at Site-B or Site-C.
- Site-B and Site-C must be able to communicate between sites and share routes using OSPF.

PE interface configuration:

```
interface FastEthernet0/0
 ip vrf forwarding Site-A
!
interface FastEthernet0/1
 ip vrf forwarding SharedSites
!
interface FastEthernet0/2
 ip vrf forwarding SharedSites
```

Which configuration meets the requirements?

```
PE(config)#router ospf 10 vrf Site-A
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0
PE(config)#router ospf 10 vrf SharedSites
PE(config-router)#network 0.0.0.0 255.255.255.255 area 1
```

```
PE(config)#router ospf 10 vrf Site-A
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0
PE(config)#router ospf 10 vrf SharedSites
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0
```

```
PE(config)#router ospf 10 vrf Site-A
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0
PE(config)#router ospf 20 vrf SharedSites
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0
```

```
PE(config)#router ospf 10 vrf Site-A
PE(config-router)#network 0.0.0.0 255.255.255.255 area 0
PE(config)#router ospf 20 vrf SharedSites
PE(config-router)#network 0.0.0.0 255.255.255.255 area 1
```

A. Option A

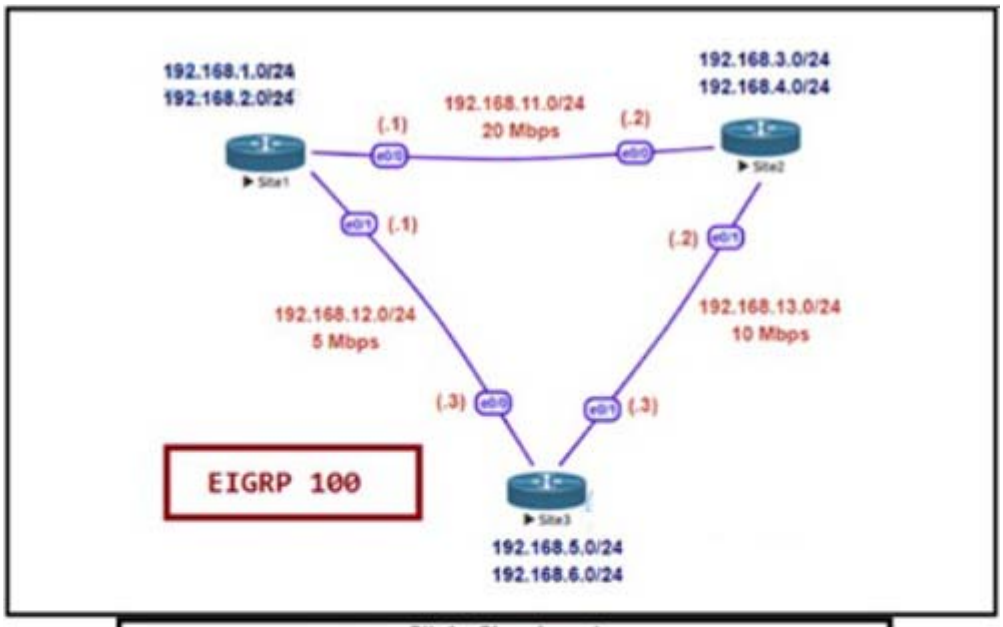
B. Option B

C. Option C

D. Option D

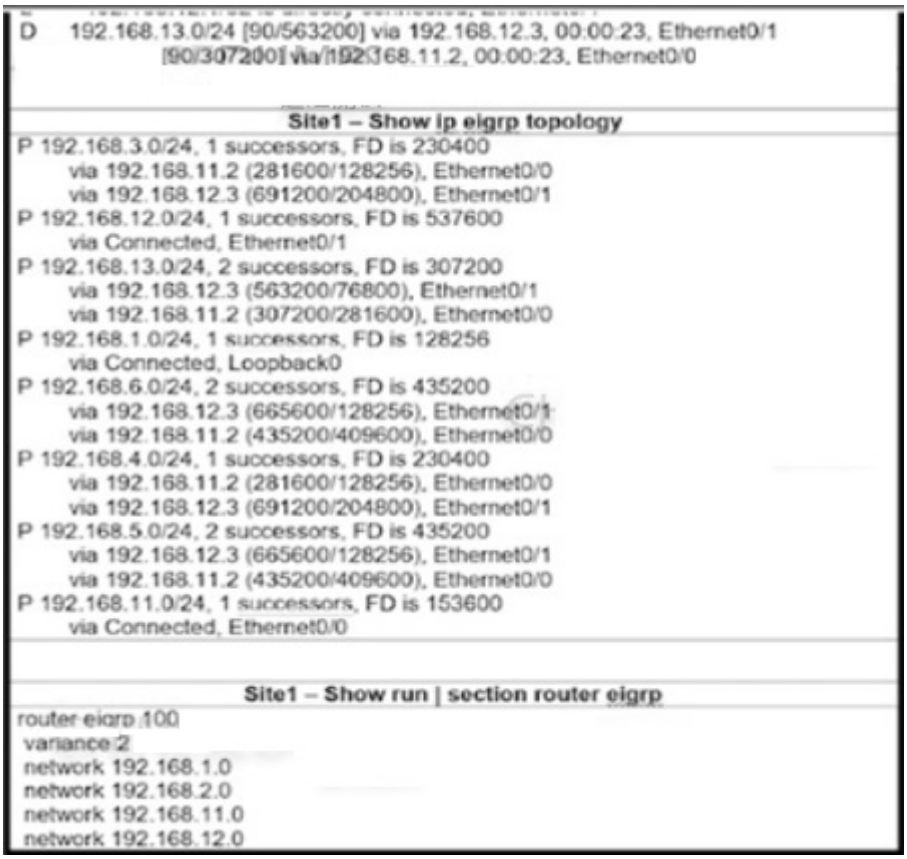
Answer: C

340.Refer to the exhibit.



Site1 – Show ip route

```
Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Loopback0
L       192.168.1.1/32 is directly connected, Loopback0
D    192.168.3.0/24 [90/281600] via 192.168.11.2, 00:00:23, Ethernet0/0
D    192.168.4.0/24 [90/281600] via 192.168.11.2, 00:00:23, Ethernet0/0
D    192.168.5.0/24 [90/665600] via 192.168.12.3, 00:00:23, Ethernet0/1
                    [90/435200] via 192.168.11.2, 00:00:23, Ethernet0/0
D    192.168.6.0/24 [90/665600] via 192.168.12.3, 00:00:23, Ethernet0/1
                    [90/435200] via 192.168.11.2, 00:00:23, Ethernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.11.0/24 is directly connected, Ethernet0/0
L       192.168.11.1/32 is directly connected, Ethernet0/0
```



Site1 must perform unequal cost load balancing toward the segments behind Site2 and Site3. Some of the routes are getting load balanced but others are not.

Which configuration allows Site1 to load balance toward all the LAN segments of the remote routers?

Site2

```
router eigrp 100
 variance 3
```

Site2

```
router eigrp 100
 variance 2
```

Site3

```
router eigrp 100
 variance 2
```

Site1

```
router eigrp 100
 variance 3
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

341.Refer to the exhibit.

```
R1:
interface Loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 10 area 0
!
interface Loopback4
 no ip address
 ipv6 address 400A:0:400C::1/64
 ipv6 enable
 ipv6 ospf 10 area 0
!
interface Serial1/0
 no ip address
 ipv6 address AB01:2011:7:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 10 area 0
 ipv6 traffic-filter DENY_TELNET_Lo4 in
 serial restart-delay 0
 clock rate 64000
!
ipv6 router ospf 10
 router-id 1.1.1.1
 log-adjacency-changes
!
ipv6 access-list DENY_TELNET_LO4
 sequence 20 deny tcp host 100:ABC:2011:7 host 400A:0:400C::1 eq telnet permit ipv6 any any
end
```

```
R2:
interface Loopback0
 no ip address
 ipv6 address 1001:ABC:2011:7::1/64
 ipv6 enable
 ipv6 ospf 10 area 0
!
interface Serial1/0
 no ip address
 ipv6 address AB01:2011:7:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 10 area 0
 serial restart-delay 0
!
ipv6 router ospf 10
 router-id 2.2.2.2
 log-adjacency-changes
!
end
```

An engineer implemented an access list on R1 to allow anyone to Telnet except R2 Loopback0 to R1 Loopback4.

How must sequence 20 be replaced on the R1 access list to resolve the issue?

A. sequence 20 permit tcp host 1001:ABC:2011:7::1 host 400A:0:400C:11 eq telnet
B. sequence 20 deny tcp host 400A:0:400C::1 host 1001:ABC:2011:7::1 eq telnet
C. sequence 20 deny tcp host 1001:ABC:2011:7::1 host 400A:0:400C::1 eq telnet
D. sequence 20 permit tcp host 400A:0:400C::1 host 1001:ABC:2011:7::1 eq telnet

Answer: C

342.An engineer notices that R1 does not hold enough log messages to Identity the root cause during troubleshooting.

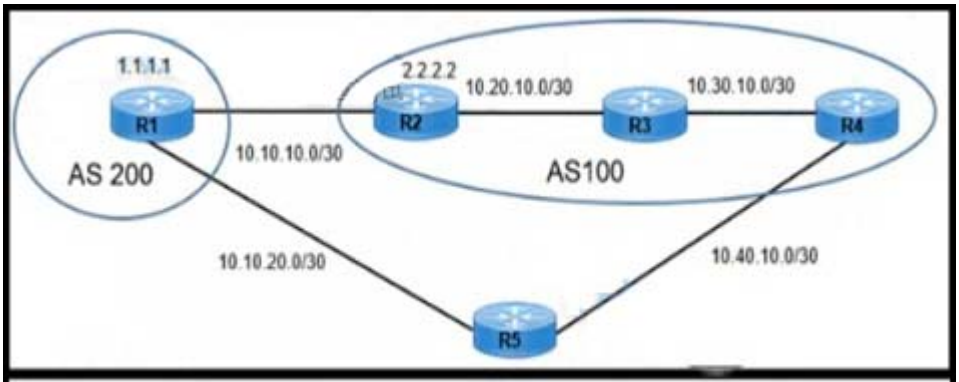
Which command resolves this issue?

- #logging buffered 4096 critical
- (config)#logging buffered 16000 informational
- #logging buffered 16000 critical
- (config)#logging buffered 4096 informational

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

343.Refer to the Exhibit.




```
R2#                                          R1#
router eigrp 100                             router eigrp 100
network 10.10.10.0 0.0.0.3                   network 10.10.10.0 0.0.0.3
network 10.20.10.0 0.0.0.3                   network 10.10.20.0 0.0.0.3
!                                            network 1.1.1.1 0.0.0.0
router ospf 100                              !
network 10.10.10.0 0.0.0.3 area 0            router ospf 100
network 10.20.10.0 0.0.0.3 area 0            network 10.10.10.0 0.0.0.3 area 0
!                                            network 10.10.20.0 0.0.0.3 area 0
!                                            !
!                                            router bgp 200
router bgp 100                               distance 100 10.10.10.0 0.0.0.3
distance 100 10.20.10.0 0.0.0.3              distance 100 10.10.10.0 0.0.0.3
distance 100 10.10.10.0 0.0.0.3              neighbor 2.2.2.2 remote-as 100
neighbor 1.1.1.1 remote-as 200               neighbor 10.10.10.2 remote-as 100
neighbor 10.10.10.1 remote-as 200            network 10.10.10.0 mask 255.255.255.252
network 10.20.10.0 mask 255.255.255.252      network 10.20.10.0 mask 255.255.255.252
```

R1 and R2 use IGP protocol to route traffic between AS 100 and AS 200 despite being configured to use BGP.

Which action resolves the issue and ensures the use of BGP?

A. Configure distance to 100 under the EIGRP process of R1 and R2.

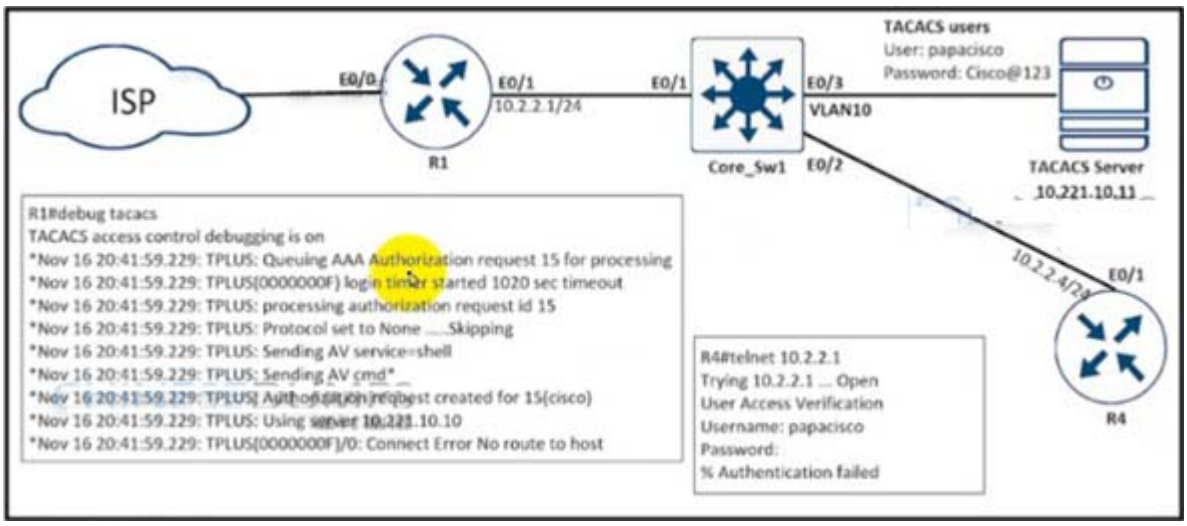
B. Remove distance commands under BGP AS 100 and AS 200.

C. Remove distance commands under BGP AS 100.

D. Configure distance to 100 under the OSPF process of R1 and R2

Answer: B

344.Refer to the exhibit.

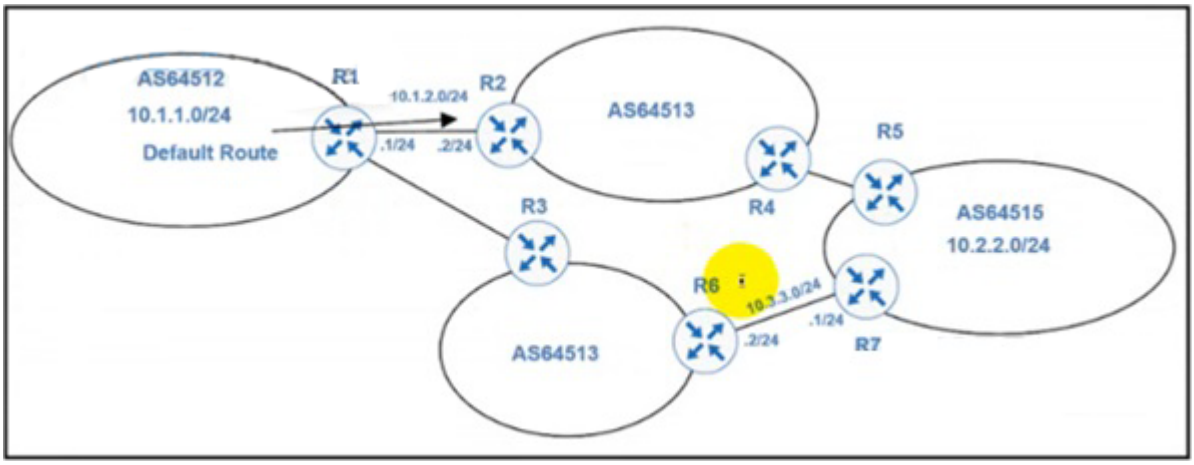


An engineer is trying to connect to R1 via Telnet with no success.
Which configuration resolves the issue?

- tacacs server prod
  address ipv4 10.221.10.10
  exit
- ip route 10.221.10.10 255.255.255.255 ethernet 0/1
- tacacs server prod
  address ipv4 10.221.10.11
  exit
- ip route 10.221.0.11 255.255.255.255 ethernet 0/1

A. Option A
B. Option B
C. Option C
D. Option D
Answer: B

345.Refer to the exhibit.



An engineer must configure PBR on R1 to reach to 10.2.2.0/24 via R3 AS64513 as the primary path and a backup route through default route via R2 AS64513. All BGP routes are in the routing table of R1. but a static default route overrides BGP routes.

Which PBR configuration achieves the objective?

```
access-list 100 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
!
route-map PBR permit 10
 match ip address 100
 set ip next-hop 10.3.3.1
```

```
access-list 100 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
!
route-map PBR permit 10
 match ip address 100
 set ip next-hop recursive 10.3.3.1
```

```
access-list 100 permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
!
route-map PBR permit 10
 match ip address 100
 set ip next-hop recursive 10.3.3.1
```

```
access-list 100 permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
!
route-map PBR permit 10
 match ip address 100
 set ip next-hop 10.3.3.1
```

A. Option A
B. Option B
C. Option C
D. Option D
Answer: B

346.Refer to the exhibit.

Configuration Output:

```
aaa new-model
aaa group server tacacs+ admin
server name admin
!
ip tacacs source-interface GigabitEthernet1
aaa authentication login admin group tacacs+ local enable
aaa session-id common
!
tacacs server admin
address ip 10.11.15.6
key 7 01150F165E1C07032D
!
line vty 0 4
login authentication admin
```

Debug Output:

```
Oct 22 12:38:57.587: AAA/BIND(0000001A): Bind i/f
Oct 22 12:38:57.587: AAA/AUTHEN/LOGIN (0000001A): Pick method list 'admin'
Oct 22 12:38:57.587: AAA/AUTHEN/ENABLE(0000001A): Processing request action LOGIN
Oct 22 12:38:57.587: AAA/AUTHEN/ENABLE(0000001A): Done status GET_PASSWORD
Oct 22 12:39:02.327: AAA/AUTHEN/ENABLE(0000001A): Processing request action LOGIN
Oct 22 12:39:02.327: AAA/AUTHEN/ENABLE(0000001A): Done status FAIL - bad password
```

An administrator configured a Cisco router for TACACS authentication, but the router is using the local

enable password instead.

Which action resolves the issue?

- Configure the **aaa authentication login admin group admin local enable** command instead.
- Configure the **aaa authentication login admin group tacacs+ local enable none** command instead.
- Configure the **aaa authentication login admin group tacacs+ local if-authenticated** command instead.
- Configure the **aaa authentication login default group admin local if-authenticated** command instead.

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

347.Refer to the exhibit.

```
Router#show ip bgp vpnv4 rd 1100:1001 10.30.116.0/23
BGP routing table entry for 1100:1001:10.30.116.0/23, version 26765275
Paths: (9 available, best #6, no table)
  Advertised to update-groups:
     1        2        3
  (65001 64955 65003) 65089, (Received from a RR-client)
    172.16.254.226 (metric 20645) from 172.16.224.236 (172.16.224.236)
      Origin IGP, metric 0, localpref 100, valid, confed-internal
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362
  (65008 64955 65003) 65089
    172.16.254.226 (metric 20645) from 10.131.123.71 (10.131.123.71)
      Origin IGP, metric 0, localpref 100, valid, confed-external
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362
  (65001 64955 65003) 65089
    172.16.254.226 (metric 20645) from 172.16.216.253 (172.16.216.253)
      Origin IGP, metric 0, localpref 100, valid, confed-external
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362
  (65001 64955 65003) 65089
    172.16.254.226 (metric 20645) from 172.16.216.252 (172.16.216.252)
      Origin IGP, metric 0, localpref 100, valid, confed-external
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362
  (64955 65003) 65089
    172.16.254.226 (metric 20645) from 10.77.255.57 (10.77.255.57)
      Origin IGP, metric 0, localpref 100, valid, confed-external
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362
  (64955 65003) 65089
    172.16.254.226 (metric 20645) from 10.57.255.11 (10.57.255.11)
      Origin IGP, metric 0, localpref 100, valid, confed-external, best
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362
```

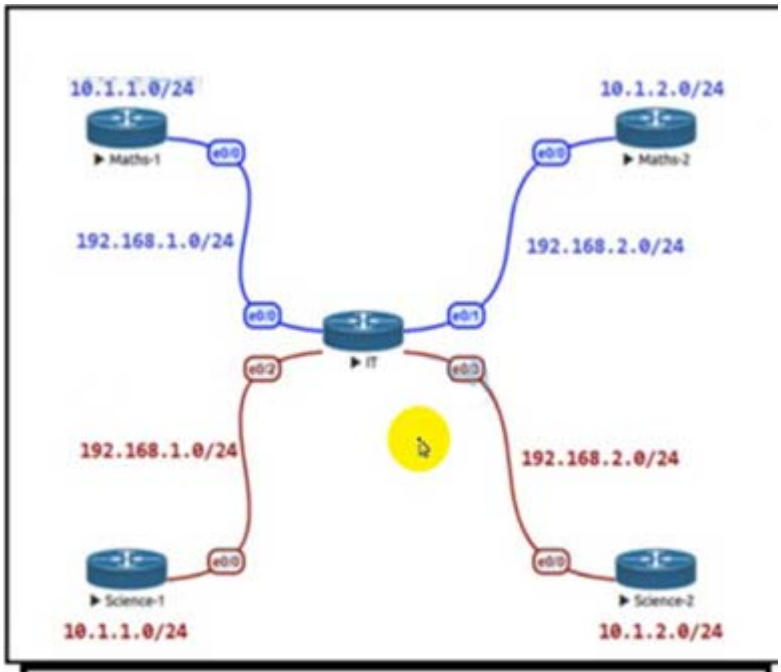
```
  (64955 65003) 65089
    172.16.254.226 (metric 20645) from 172.16.224.253 (172.16.224.253)
      Origin IGP, metric 0, localpref 100, valid, confed-internal
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362
  (65003) 65089
    172.16.254.226 (metric 20645) from 172.16.254.234 (172.16.254.234)
      Origin IGP, metric 0, localpref 100, valid, confed-external
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/362
  65089, (Received from a RR-client)
    172.16.228.226 (metric 20645) from 172.16.228.226 (172.16.228.226)
      Origin IGP, metric 0, localpref 100, valid, confed-internal
      Extended Community: RT:1100:1001
      mpls labels in/out nolabel/278
```

An engineer configured BGP and wants to select the path from 10.77.255.57 as the best path instead of current best path.
Which action resolves the issue?
A. Configure AS_PATH prepend for the desired best path
B. Configure higher MED to select as the best path.
C. Configure lower LOCAL_PREF to select as the best path.
D. Configure AS_PATH prepend for the current best path
Answer: D

348.What is LDP label binding?
A. neighboring router with label
B. source prefix with label
C. destination prefix with label
D. two routers with label distribution session
Answer: C
Explanation:
For every IGP IP prefix in its IP routing table, each LSR creates a local binding—that is, it binds a label to the IPv4 prefix. The LSR then distributes this binding to all its LDP neighbors. These received bindings become remote bindings. The neighbors then store these remote and local bindings in a special table, the label information base (LIB). Each LSR has only one local binding

349.Which table is used to map the packets in an MPLS LSP that exit from the same interface, via the same next hop, and have the same queuing policies?
A. RIB
B. FEC
C. LDP
D. CEF
Answer: B

350.Refer to the exhibit.



IT Router

```
vrf definition Science
 address-family ipv4
!
Interface E 0/2
 Vrf forwarding Science
 Ip address 192.168.1.1 255.255.255.0
 No shut
!
Interface E 0/3
 Vrf forwarding Science
!
Interface E 0/3
 Vrf forwarding Science
 Ip address 192.168.2.1 255.255.255.0
 No shut
```

The IT router has been configured with the Science VRF and the interfaces have been assigned to the VRF.

Which set of configurations advertises Science-1 and Science-2 routes using EIGRPAS 111?

```
router eigrp 111
 address-family ipv4 vrf Science autonomous-system 1
 network 192.168.1.0
 network 192.168.2.0

router eigrp 111
 address-family ipv4 vrf Science
 network 192.168.1.0
 network 192.168.2.0

router eigrp 111
 network 192.168.1.0
 network 192.168.2.0

router eigrp 1
 address-family ipv4 vrf Science autonomous-system 111
 network 192.168.1.0
 network 192.168.2.0
```

A. Option A

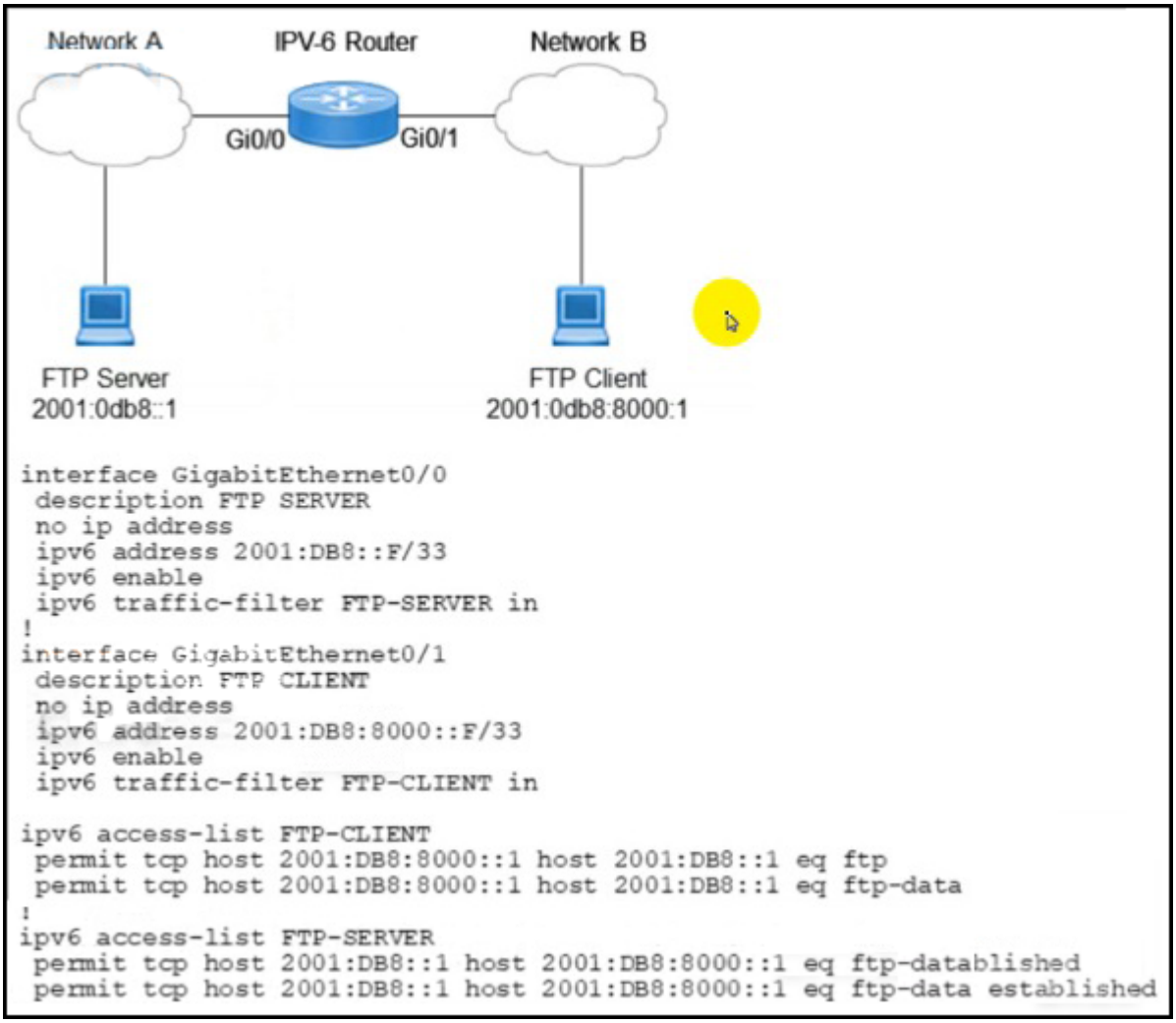
B. Option B

C. Option C

D. Option D

Answer: D

351.Refer to the exhibit.

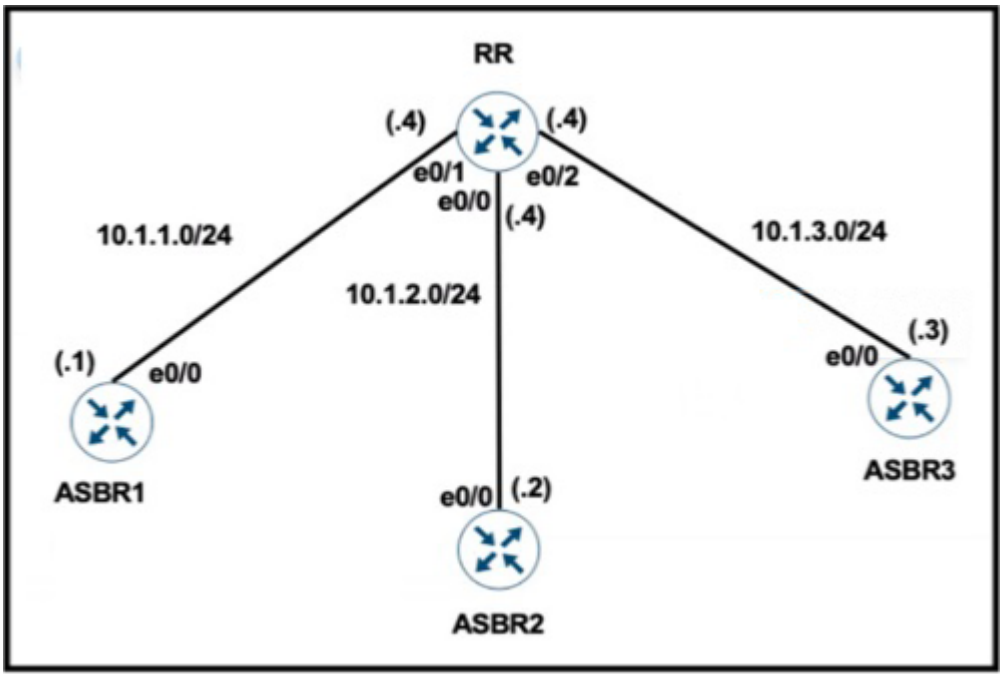


When an FTP client attempts to use passive FTP to connect to the FTP server, the file transfers fail.

Which action resolves the issue?
A. Configure active FTP traffic.
B. Modify FTP-SERVER access list to remove established at the end.
C. Modify traffic filter FTP-SERVER in to the outbound direction.
D. Configure to permit TCP ports higher than 1023.
Answer: D

352.In a DMVPN network, the Spoke1 user observed that the voice traffic is coming to Spoke2 users via the hub router.
Which command is required on both spoke routers to communicate directly to one another?
A. ip nhrp map dynamic
B. ip nhrp shortcut
C. ip nhrp nhs multicast
D. ip nhrp redirect
Answer: B

353.Refer to the exhibit.



RR Configuration:

```
router bgp 100
 neighbor IBGP peer-group
 neighbor IBGP route-reflector-client
 neighbor 10.1.1.1 remote-as 100
 neighbor 10.1.2.2 remote-as 100
 neighbor 10.1.3.3 remote-as 100
```

The network administrator configured the network to establish connectivity between all devices and notices that the ASBRs do not have routes for each other.
Which set of configurations resolves this issue?

router bgp 100
neighbor 10.1.1.1 next-hop-self
neighbor 10.1.2.2 next-hop-self
neighbor 10.1.3.3 next-hop-self

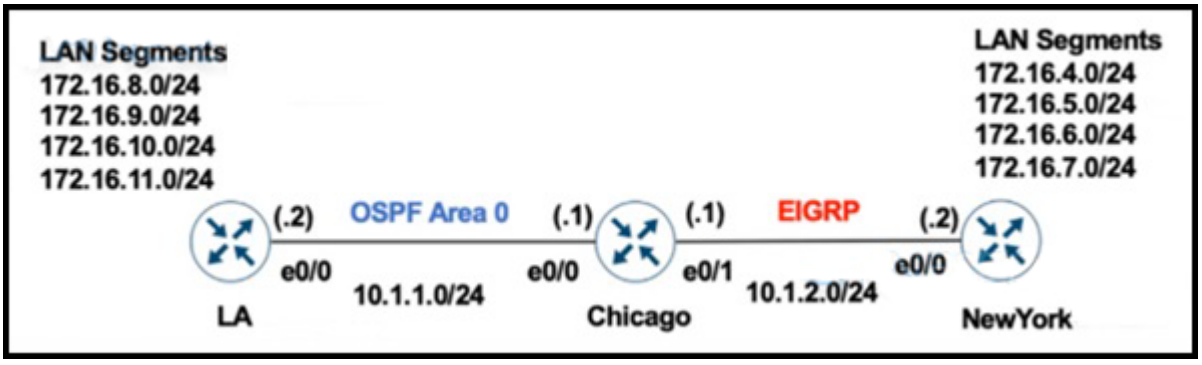
router bgp 100
neighbor IBGP update-source Loopback0

router bgp 100
neighbor IBGP next-hop-self

router bgp 100
neighbor 10.1.1.1 peer-group IBGP
neighbor 10.1.2.2 peer-group IBGP
neighbor 10.1.3.3 peer-group IBGP

A. Option A
B. Option B
C. Option C
D. Option D
Answer: D

354.Refer to the exhibit.



The network administrator configured the Chicago router to mutually redistribute the LA and NewYork routes with OSPF routes to be summarized as a single route in EIGRP using the longest summary mask:

```
router eigrp 100
 redistribute ospf 1 metric 10 10 10 10 10
router ospf 1
 redistribute eigrp 100 subnets
!
interface E 0/0
 ip summary-address eigrp 100 172.16.0.0 255.255.0.0
```

After the configuration, the New York router receives all the specific LA routes but the summary route. Which set of configurations resolves the issue on the Chicago router?

interface E 0/1
ip summary-address eigrp 100 172.16.0.0 255.255.0.0

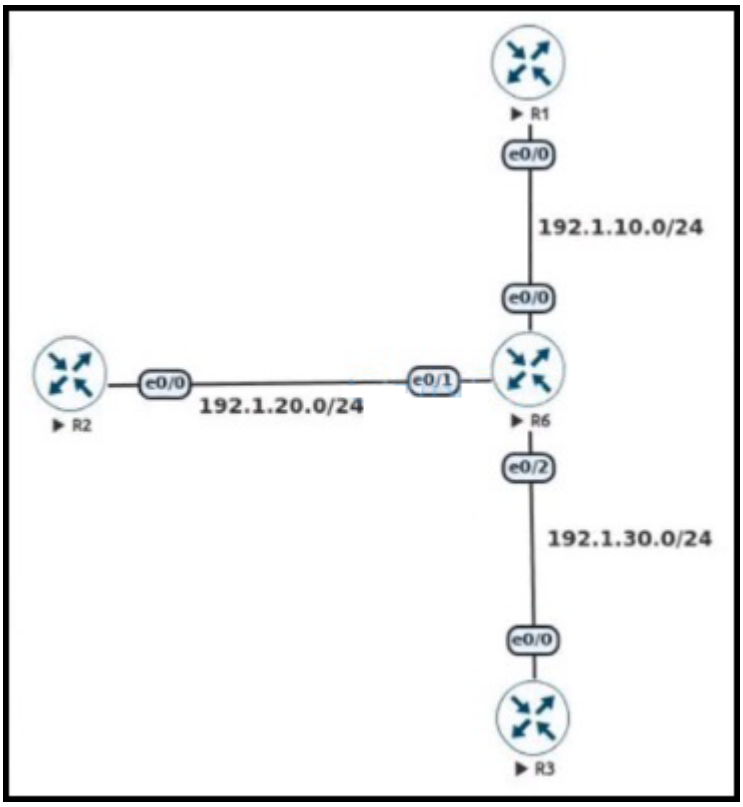
interface E 0/1
ip summary-address eigrp 100 172.16.8.0 255.255.252.0

router eigrp 100
summary-address 172.16.8.0 255.255.252.0

router eigrp 100
summary-address 172.16.0.0 255.255.0.0

A. Option A
B. Option B
C. Option C
D. Option D
Answer: B

355.Refer to the exhibit.



An engineer must configure DMVPN Phase 3 hub-and-spoke topology to enable a spoke-to-spoke tunnel.
Which NHRP configuration meets the requirement on R6?

```
Interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source e 0/0
 tunnel mode gre multipoint
 ip nhrp network-id 1

interface Tunnel1
 ip nhrp authentication Cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp holdtime 300
 ip nhrp redirect

interface Tunnel1
 ip nhrp authentication Cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp holdtime 300
 ip nhrp shortcut

Interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source e 0/1
 tunnel mode gre multipoint
 ip nhrp network-id 1
 ip nhrp map 192.168.1.2 192.1.20.2
```

A. Option A

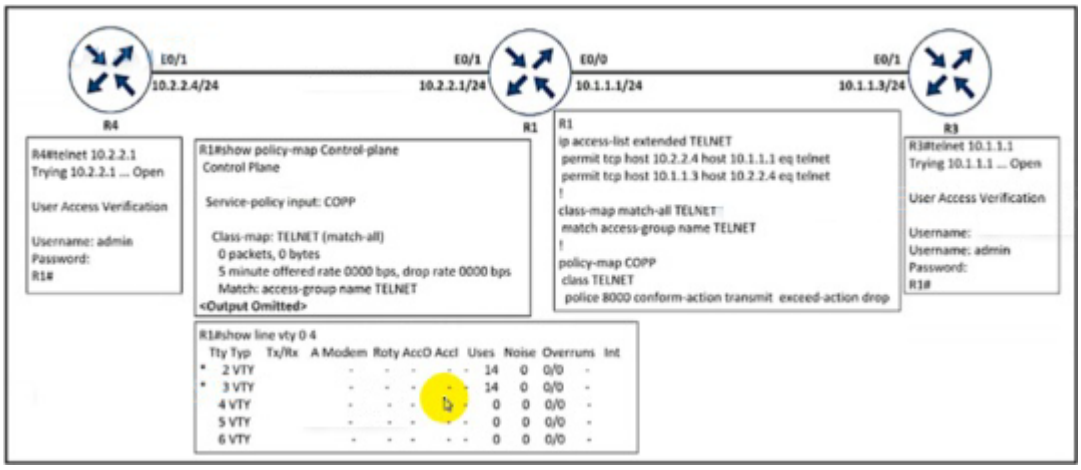
B. Option B

C. Option C

D. Option D

Answer: B

356.Refer to the exhibit.



An engineer implemented CoPP to limit Telnet traffic to protect the router CPU. It was noticed that the Telnet traffic did not pass through CoPP.

Which configuration resolves the issue?

```
policy-map COPP
 class TELNET
  police 8000 conform-action transmit  exceed-action transmit
```

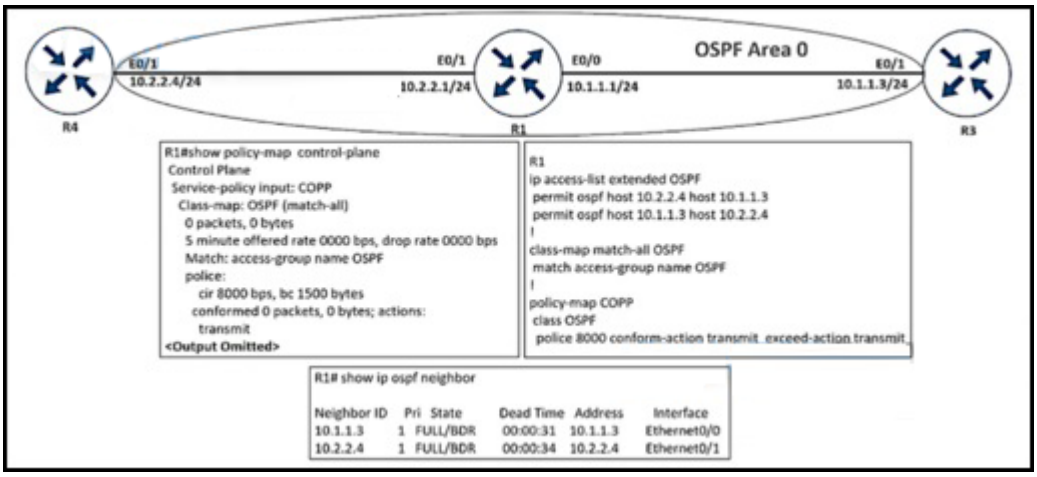
```
policy-map COPP
 class TELNET
  police 8000 conform-action transmit  exceed-action transmit  violate-action drop
```

```
ip access-list extended TELNET
 permit tcp host 10.2.2.1 host 10.2.2.4 eq telnet
 permit tcp host 10.1.1.1 host 10.1.1.3 eq telnet
```

```
ip access-list extended TELNET
 permit tcp host 10.2.2.4 host 10.2.2.1 eq telnet
 permit tcp host 10.1.1.3 host 10.1.1.1 eq telnet
```

A. Option A
B. Option B
C. Option C
D. Option D
Answer: D

357.Refer to the exhibit.



An engineer implemented CoPP but did not see OSPF traffic going through it.
Which configuration resolves the issue?

```
ip access-list extended OSPF
 permit ospf any any
```

```
policy-map COPP
 class OSFP
  police 8000 conform-action transmit  exceed-action transmit  violate-action drop
```

```
control-plane
 service-policy input COPP
```

```
class-map match-all OSFP
 match access-group name OSPF
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

358.An engineer must override the normal routing behavior of a router for Telnet traffic that is destined to 10.10.10.10 from 10.10.1.0/24 via a next hop of 10.4.4.4. which is directly connected to the router that is connected to the 10.1.1.0/24 subnet.
Which configuration reroutes traffic according to this requirement?

```
access-list 100 permit tcp 10.10.1.0 0.0.0.255 host 10.10.10.10 eq 23
!
route-map POLICY permit 10
 match ip address 100
 set ip next-hop recursive 10.4.4.4
```

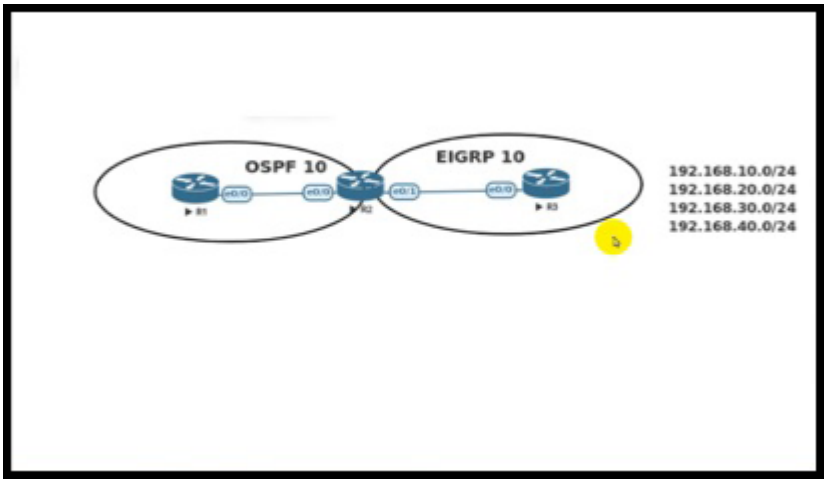
```
access-list 100 permit tcp 10.10.1.0 0.0.0.255 host 10.10.10.10 eq 23
!
route-map POLICY permit 10
 match ip address 100
 set ip next-hop 10.4.4.4
route-map POLICY permit 20
```

```
access-list 100 deny tcp 10.10.1.0 0.0.0.255 host 10.10.10.10 eq 23
!
route-map POLICY permit 10
 match ip address 100
 set ip next-hop 10.4.4.4
route-map POLICY permit 20
```

```
access-list 100 permit tcp 10.10.1.0 0.0.0.255 hodt 10.10.10.10 eq 23
!
route-map POLICY permit 10
 match ip address 100
 set ip next-hop recursive 10.4.4.4
route-map POLICY permit 20
```

A. Option A
B. Option B
C. Option C
D. Option D
Answer: B

359.Refer to the exhibit.



An engineer must redistribute networks 192.168.10.0/24 and 192.168.20.0/24 into OSPF from EIGRP. where the metric must be added when traversing through multiple hops to start an external route of 20 The engineer notices that the external metric is fixed and does not add at each hop.
Which configuration resolves the issue?

```
R2(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R2(config)#access-list 10 permit 192.168.20.0 0.0.0.255
!
R2(config)#route-map RD permit 10
R2(config-route-map)#match ip address 10
R2(config-route-map)#set metric 20
R2(config-route-map)#set metric-type type-2
!
R2(config)#router ospf 10
R2(config-router)#redistribute eigrp 10 subnets route-map RD
```

```
R2(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R2(config)#access-list 10 permit 192.168.20.0 0.0.0.255
!
R2(config)#route-map RD permit 10
R2(config-route-map)#match ip address 10
R2(config-route-map)#set metric 20
R2(config-route-map)#set metric-type type-1
!
R2(config)#router ospf 10
R2(config-router)#redistribute eigrp 10 subnets route-map RD
```

```
R1(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#access-list 10 permit 192.168.20.0 0.0.0.255
!
R1(config)#route-map RD permit 10
R1(config-route-map)#match ip address 10
R1(config-route-map)#set metric 20
R1(config-route-map)#set metric-type type-1
!
R1(config)#router ospf 10
R1(config-router)#redistribute eigrp 10 subnets route-map RD
```

```
R1(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#access-list 10 permit 192.168.20.0 0.0.0.255
!
R1(config)#route-map RD permit 10
R1(config-route-map)#match ip address 10
R1(config-route-map)#set metric 20
R1(config-route-map)#set metric-type type-2
!
R1(config)#router ospf 10
R1(config-router)#redistribute eigrp 10 subnets route-map RD
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: B

360.An administrator attempts to download the pack NBAR2 file using TFTP from the CPE router to another device over the Gi0/0 interface.

The CPE is configured as below:

```
hostname CPE
!
ip access-list extended WAN
<...>
remark => All UDP rules below for WAN ID: S420T92E35F99
permit udp any eq domain any
permit udp any any eq tftp
deny udp any any
!
interface GigabitEthernet0/0
<...>
ip access-group WAN in
<...>
!
tftp-server flash:pp-adv-csr1000v-1612.1a-37-53.0.0.pack
```

The transfer fails.
Which action resolves the issue?
A. Change the WAN ACL to permit the UDP port 69 to allow TFTP
B. Make the permit udp any eq tftp any entry the last entry in the WAN ACL.
C. Change the WAN ACL to permit the entire UDP destination port range
D. Shorten the file name to the 8+3 naming convention.
Answer: B

361.What is an MPLS LDP targeted session?
A. session between neighbors that are connected no more than one hop away
B. LDP session established between LSRs by exchanging TCP hello packets
C. label distribution session between non-directly connected neighbors
D. LDP session established by exchanging multicast hello packets
Answer: C

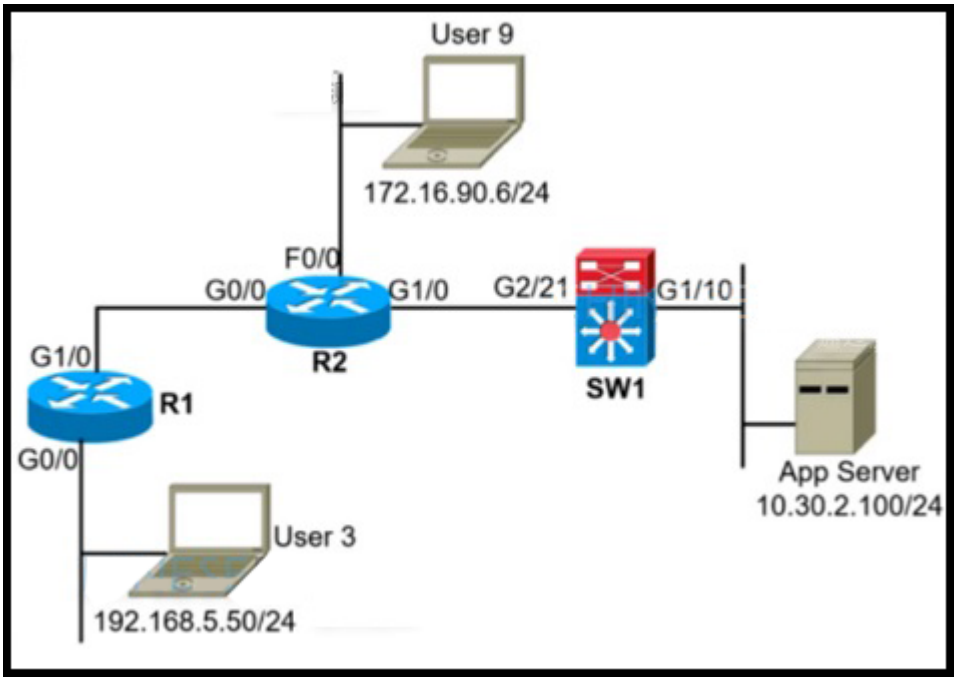
362.Refer to the exhibit.

```
ip sla 1
 icmp-echo 8.8.8.8
 threshold 1000
 timeout 2000
 frequency 5
ip sla schedule 1 life forever start-time now
!
track 1 ip sla 1
!
ip route 0.0.0.0 0.0.0.0 203.0.113.1 name ISP1 track 1
ip route 0.0.0.0 0.0.0.0 198.51.100.1 name ISP2 track 1
```

An administrator configures a router to stop using a particular default route if the DNS server 8.8.8.8 is not reachable through that route. However, this configuration did not work as desired and the default route still works even if the DNS server 8.8.8 8 is unreachable.
Which two configuration changes resolve the issue? (Choose two.)
A. Configure two static routes for the 8.8.8.8/32 destination to match the IP SLA probe for each ISP.
B. Associate every IP SLA probe with the proper WAN address of the router.
C. Reference the proper exit interfaces along with the next hops in both static default routes.
D. Use a separate track object to reference the existing IP SLA 1 probe for every static route.

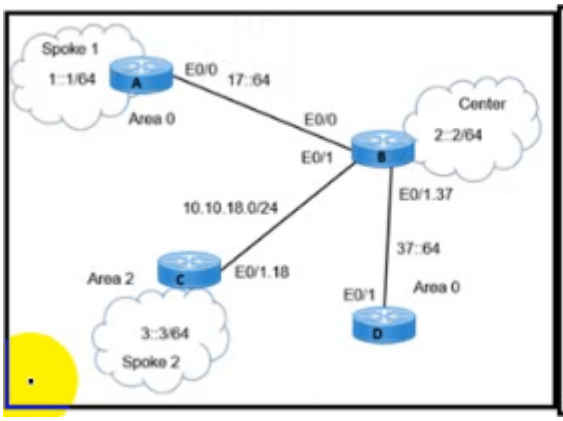
E. Use a separate IP SLA probe and track object for every static route
Answer: A E

363.Refer to the exhibit.



A network administrator must block ping from user 3 to the App Server only. An inbound standard access list is applied to R1 interface G0/0 to block ping. The network administrator was notified that user 3 cannot even ping user 9 anymore.
Where must the access list be applied in the outgoing direction to resolve the issue?
A. R2 interface G1/0
B. R2 interface GO/0
C. SW1 interface G1/10
D. SW1 interface G2/21
Answer: D

364.Refer to the exhibit.




```
B(config-if)# do sh run int e0/1 | b int
B(config-if)# interface Ethernet0/1
B(config-if)# ip address 78.1.1.8 255.255.255.0
B(config-if)# ipv6 enable
B(config-if)# ospfv3 1 ipv4 area 1

C(config)# interface Ethernet0/1.78
C(config-subif)# encap dot1q 78
C(config-subif)# ip add 78.1.1.7 255.255.255.0
C(config-subif)# ospfv3 1 ipv4 area 0

D(config-if)# do sh run int e0/1 | b int
D(config-if)# interface Ethernet0/1
D(config-if)# no ip address
D(config-if)# ipv6 address 37::3/64
D(config-if)# ipv6 enable
D(config-if)# ipv6 ospf 1 area 0
```

A network engineer receives a report that Spoke 1 users can perform bank transactions with the server located at the Center site, but Spoke 2 users cannot.

Which action resolves the issue?

A. Configure the Spoke 2 users IP on the router B OSPF domain

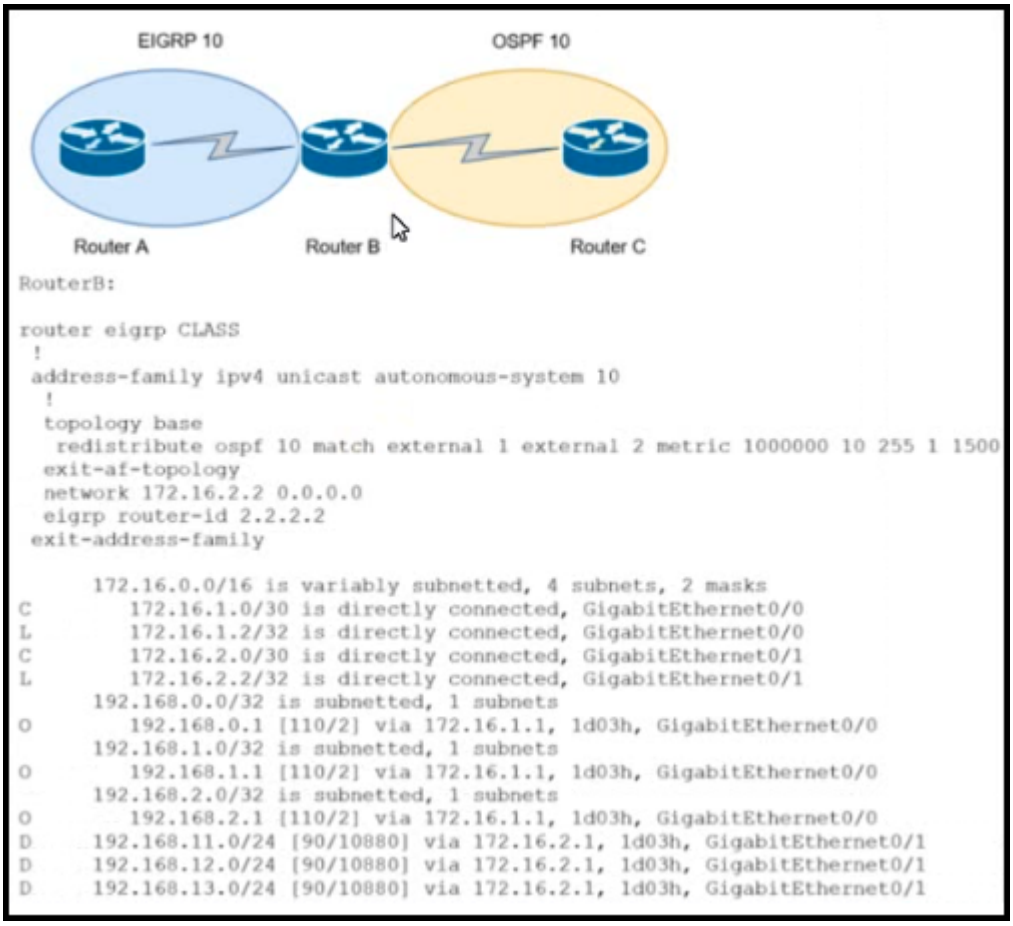
B. Configure encapsulation dot1q 78 on the router C interface.

C. Configure IPv6 on the routers B and C interfaces

D. Configure OSPFv2 on the routers B and C interfaces

Answer: C

365.Refer to the exhibit.



An engineer configured route exchange between two different companies for a migration project EIGRP routes were learned in router C but no OSPF routes were learned in router A.

Which configuration allows router A to receive OSPF routes?

(config-router-af)#**redistribute ospf 10 1000000 10 255 1 1500**

(config-router-af-topology)#**redistribute ospf 10 metric 1000000 10 255 1 1500**

(config-router-af-topology)#**redistribute connected**

(config-router-af-topology)#**no redistribute ospf 10 match external 1 external 2 metric 1000000 10 255 1 1500**

A. Option A

B. Option B

C. Option C

D. Option D

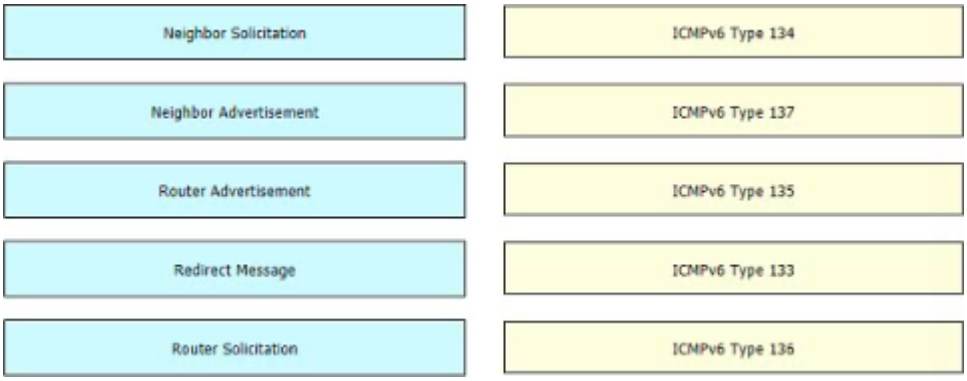
Answer: B

366.A network administrator cannot connect to a device via SSH.
The line vty configuration is as follows:

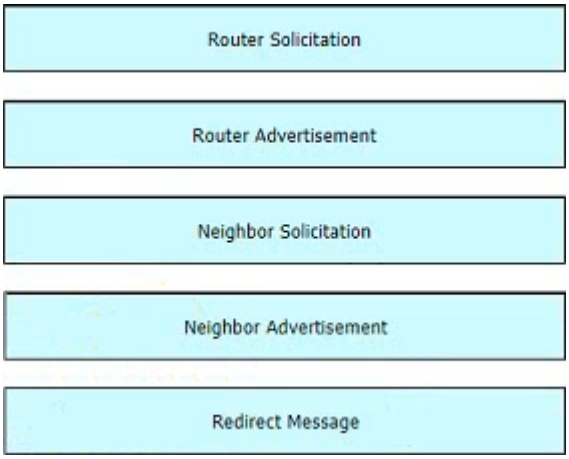
```
line vty 0 4
 location S421T50E27F86
 session-timeout 10
 transport preferred ssh
 transport input all
 transport output telnet ssh
 stopbits 1
```

Which action resolves this issue?
A. Increase the session timeout
B. Change the stopbits to 10.
C. Configure the transport input SSH
D. initialize the SSH key
Answer: D

367.DRAG DROP
Drag and drop the ICMPv6 neighbor discovery messages from the left onto the correct packet types on the right.



Answer:



368.DRAG DROP
Drag and drop the descriptions from the left onto the corresponding MPLS components on the right.

FEC	routers in the core of the provider network known as P routers
LSP	all traffic to be forwarded using the same path and same label
LER	routers that connect to the customer routers known as PE routers
LSR	used for exchanging label mapping information between MPLS enabled routers
LDP	path along which the traffic flows across an MPLS network

Answer:

FEC	LSR
LSP	FEC
LER	LER
LSR	LDP
LDP	LSP

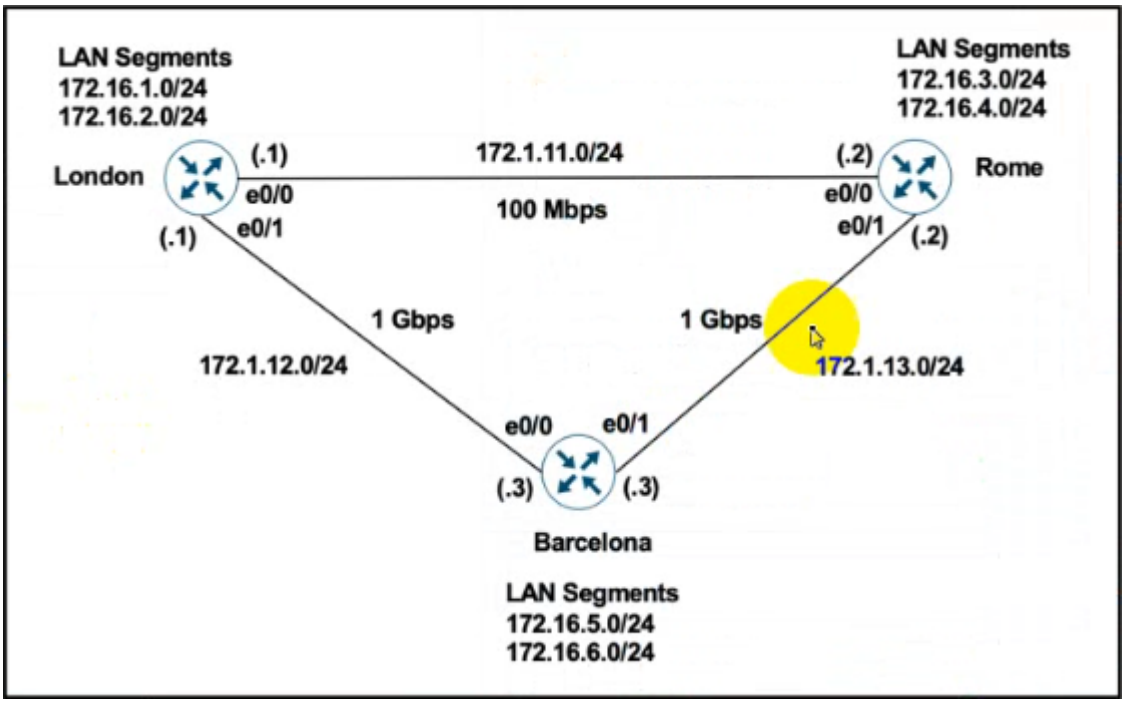
369.Refer to the exhibits.

London – "show ip route" output

```
Gateway of last resort is not set

     172.1.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.1.11.0/24 is directly connected, Ethernet0/0
L       172.1.11.1/32 is directly connected, Ethernet0/0
C       172.1.12.0/24 is directly connected, Ethernet0/1
L       172.1.12.1/32 is directly connected, Ethernet0/1
D       172.1.13.0/24 [90/76800] via 172.1.11.2, 00:00:50, Ethernet0/0
     172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
C       172.16.1.0/24 is directly connected, Loopback0
L       172.16.1.1/32 is directly connected, Ethernet0/0
C       172.16.2.0/24 is directly connected, Loopback1
L       172.16.2.1/32 is directly connected, Loopback1
R       172.16.3.0/24 [120/1] via 172.1.11.2, 00:00:08, Ethernet0/0
R       172.16.4.0/24 [120/1] via 172.1.11.2, 00:00:08, Ethernet0/0
D       172.16.5.0/24 [90/156160] via 172.1.12.3, 00:00:50, Ethernet0/1
D       172.16.6.0/24 [90/156160] via 172.1.12.3, 00:00:50, Ethernet0/1
```

Rome - "show run | section router" output

```
router eigrp 111
  network 172.1.0.0
  network 172.16.0.0
  no auto-summary
```



London must reach Rome using a faster path via EIGRP if all the links are up but it failed to take this path.

Which action resolves the issue?

A. Increase the bandwidth of the link between London and Barcelona

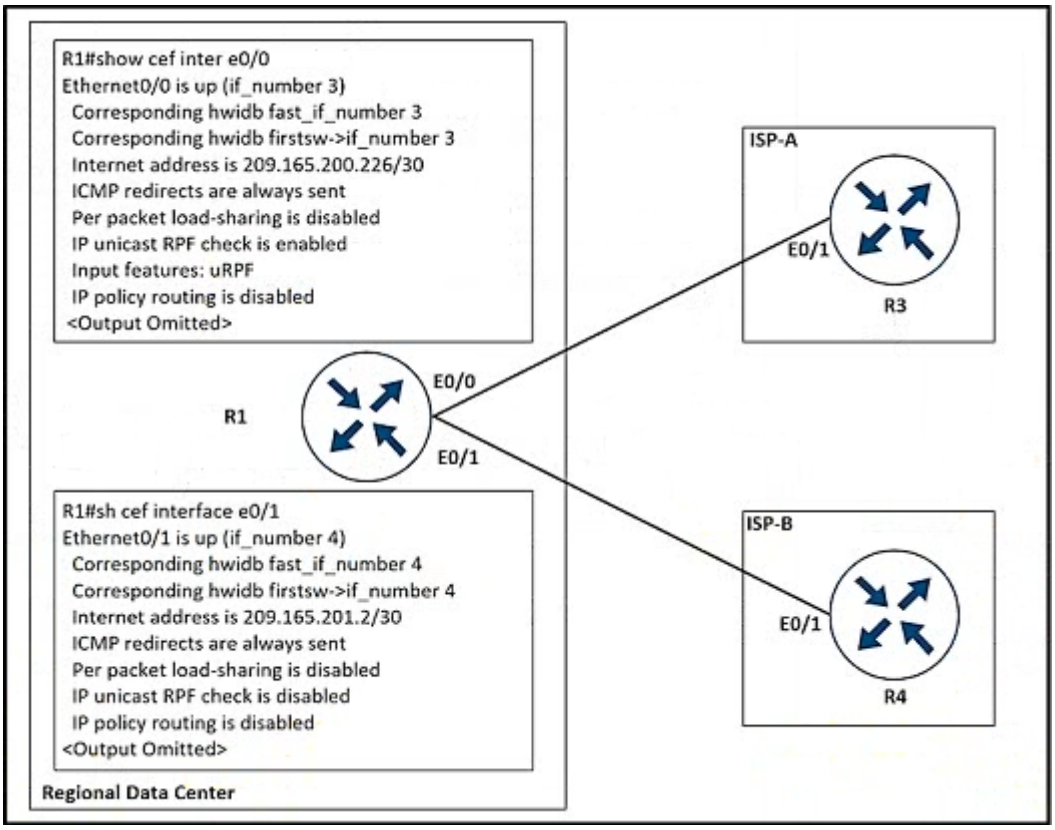
B. Use the network statement on London to inject the 172 16 X 0/24 networks into EIGRP.

C. Change the administrative distance of RIP to 150

D. Use the network statement on Rome to inject the 172 16 X 0/24 networks into EIGRP

Answer: D

370.Refer to the exhibit.



The company implemented uRPF to address an antispoofing attack. A network engineer received a call from the IT security department that the regional data center is under an IP attack.
Which configuration must be implemented on R1 to resolve this issue?

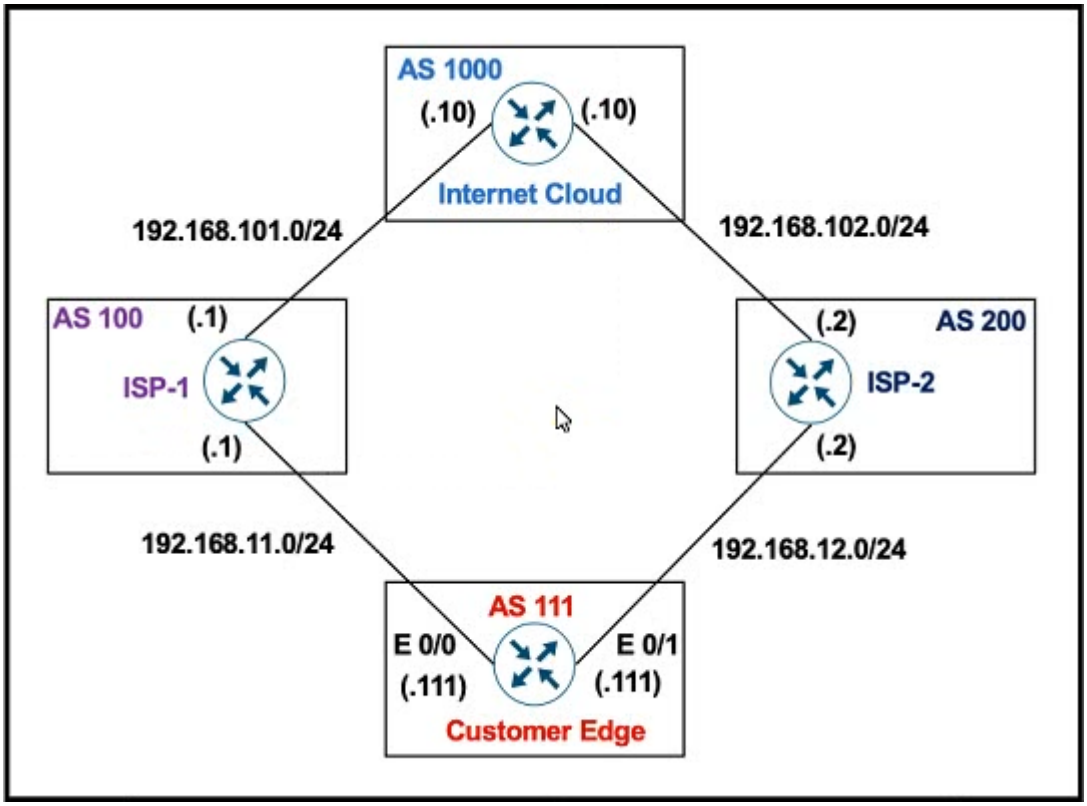
- interface ethernet0/0
  ip verify unicast reverse-path
- interface ethernet0/1
  ip verify unicast reverse-path
- interface ethernet0/1
  ip unicast RPF check reachable-via any allow-default allow-self-ping
- interface ethernet0/0
  ip unicast RPF check reachable-via any allow-default allow-self-ping

A. Option A
B. Option B
C. Option C
D. Option D
Answer: B

371.What is a function of BFD?
A. peer recovery after a Layer 3 protocol adjacency failure
B. peer recovery after a Layer 2 adjacency failure
C. failure detection independent of routing protocols and media types
D. failure detection dependent on routing protocols and media types

Answer: D

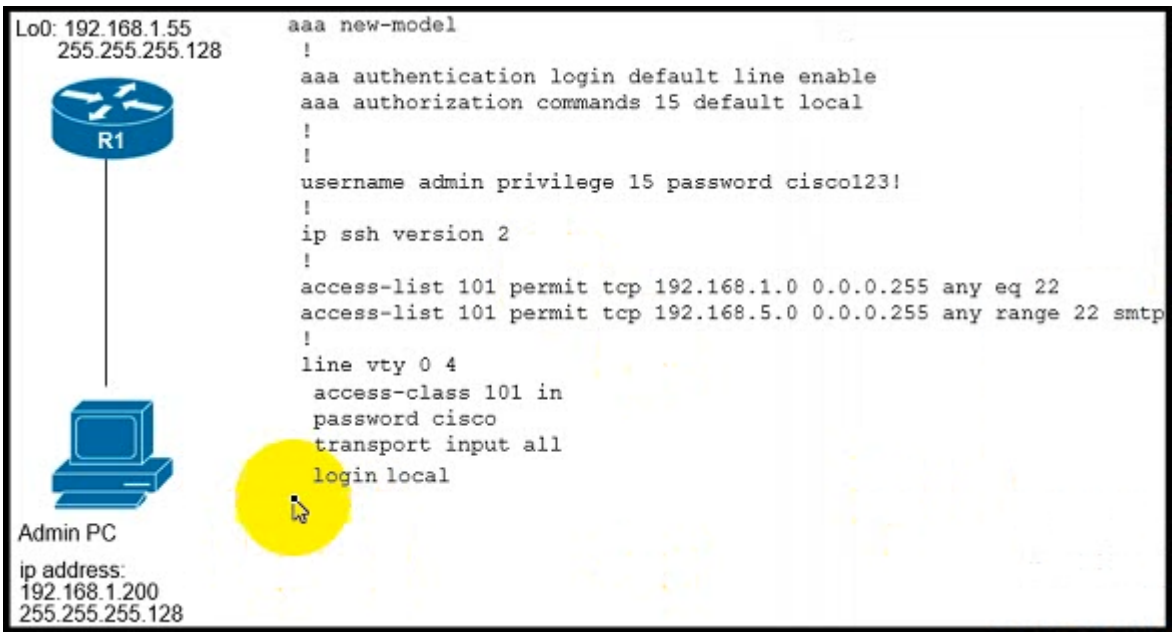
372.Refer to the exhibit.




```
ISP-1

ip as-path access-list 1 permit ^111
!
router bop 100
 neighbor 192.168.101.10 remote-as 1000
 neighbor 192.168.11.111 remote-as 111
 neighbor 192.168.11.111 filter-list 1 in
```

AS 111 mut not be used as a transit AS, but ISP-1 is getting ISP-2 routes from AS 111.
Which configuration stops Customer AS from being used as a transit path on ISP-1?
A. ip as-path access-list 1 permit ^$
B. ip as-path access-list 1 permit_111_
C. ip as-path access-list 1 permit."
D. ip as-path access-list 1 permit ^111$
Answer: A

373.Refer to the exhibit.



An engineer configured user login based on authentication database on the router, but no one can log into the router.

Which configuration resolves the issue?

A. aaa authentication login default enable

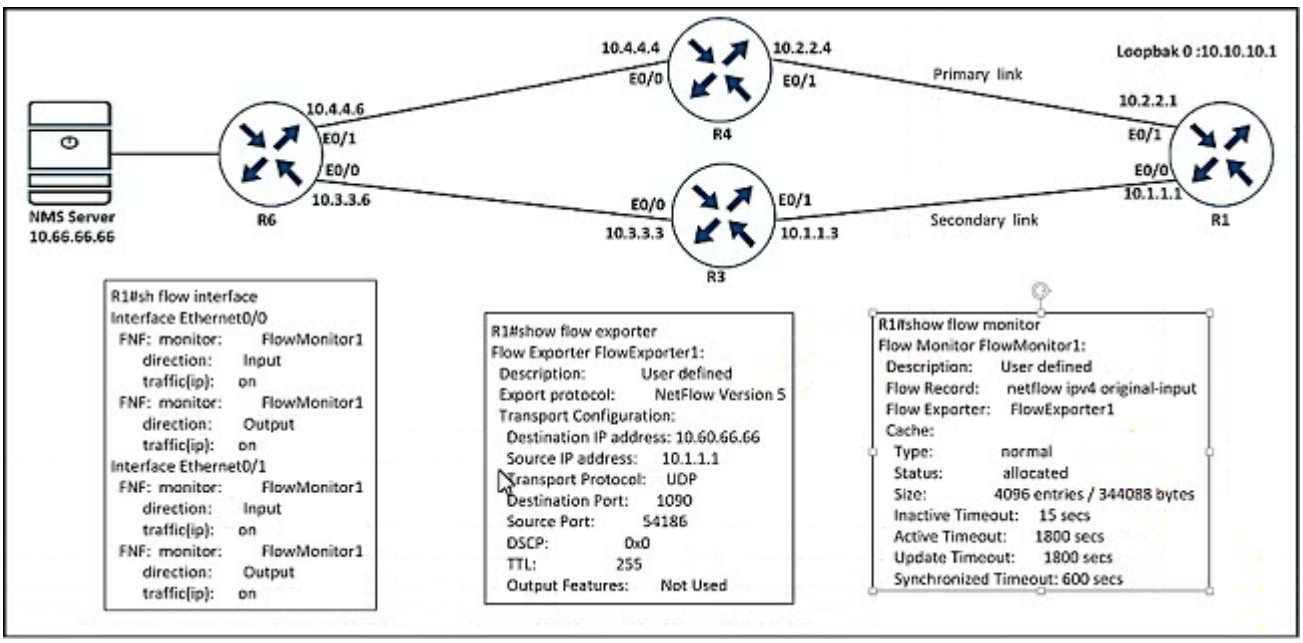
B. aaa authorization network default local

C. aaa authentication login default local

D. aaa authorization exec default local

Answer: C

374.Refer to the exhibit.



An engineer configured NetFlow on R1, but the flows do not reach the NMS server from R1.

Which configuration resolves this Issue?

R1(config)#**flow monitor FlowMonitor1**
R1(config-flow-monitor)#**destination 10.66.66.66**

R1(config)#**flow exporter FlowExporter1**
R1(config-flow-exporter)#**destination 10.66.66.66**

R1(config)#**interface Ethernet0/0**
R1(config-if)#**ip flow monitor Flowmonitor1 input**
R1(config-if)#**ip flow monitor Flowmonitor1 output**

R1(config)#**interface Ethernet0/1**
R1(config-if)#**ip flow monitor Flowmonitor1 input**
R1(config-if)#**ip flow monitor Flowmonitor1 output**

A. Option A

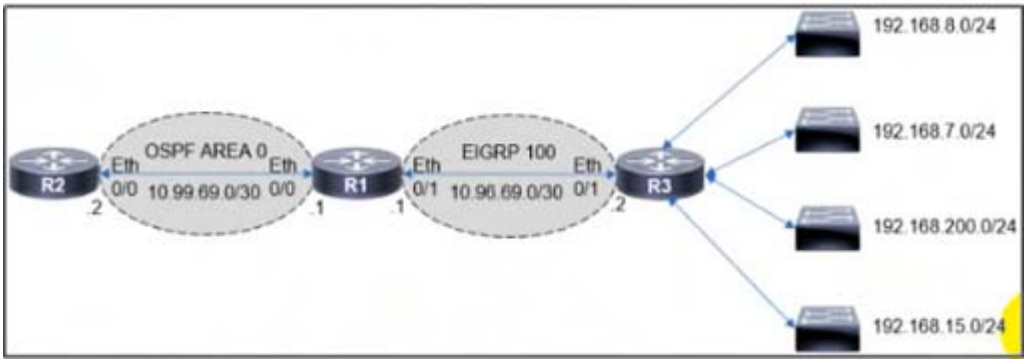
B. Option B

C. Option C

D. Option D

Answer: B

375.Refer to the exhibit.




```
R1#show route-map
route-map FROM->EIGRP, permit, sequence 10
  Match clauses:
    ip address (access-lists): 10
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
R1#show run | sec router
router eigrp 100
 network 10.96.69.0 0.0.0.3
 no auto-summary
 eigrp router-id 1.1.1.1
router ospf 100
 router-id 1.1.1.1
 log-adjacency-changes
 redistribute eigrp 100 subnets route-map FROM->EIGRP
 network 10.99.69.0 0.0.0.3 area 0
R1#show ip access-list
Standard IP access list 10
    10 permit 192.168.16.0, wildcard bits 0.0.3.255
    11 permit 192.168.0.0, wildcard bits 0.0.7.255
    20 deny   any
```

The engineer configured route redistribution in the network but soon received reports that R2 cannot access 192 168 7 0/24 and 192 168 15 0/24 subnets.

Which configuration resolves the issue?

```
R1(config)#ip access-list standard 10
R1(config-std-nacl)#no 10 permit
R1(config-std-nacl)#no 11 permit
R1(config-std-nacl)#10 permit 192.168.0.0 0.0.3.255
R1(config-std-nacl)#11 permit 192.168.8.0 0.0.3.255
```

```
R1(config)#ip access-list standard 10
R1(config-std-nacl)#no 10 permit
R1(config-std-nacl)#no 11 permit
R1(config-std-nacl)#10 permit 192.168.0.0 0.0.7.255
R1(config-std-nacl)#11 permit 192.168.8.0 0.0.3.255
```

```
R1(config)#ip access-list standard 10
R1(config-std-nacl)#no 10 permit
R1(config-std-nacl)#no 11 permit
R1(config-std-nacl)#10 permit 192.168.0.0 0.0.3.255
R1(config-std-nacl)#11 permit 192.168.8.0 0.0.7.255
```

```
R1(config)#ip access-list standard 10
R1(config-std-nacl)#no 10 permit
R1(config-std-nacl)#no 11 permit
R1(config-std-nacl)#10 permit 192.168.4.0 0.0.3.255
R1(config-std-nacl)#11 permit 192.168.12.0 0.0.3.255
```

A. Option A
B. Option B
C. Option C
D. Option D
Answer: D

376.An engineer received a ticket about a router that has reloaded. The monitoring system graphs show different traffic patterns between logical and physical interfaces when the router is rebooted.
Which action resolves the issue?
A. Configure the snmp ifindex persist command globally.
B. Clear the logical interfaces with snmp ifindex clear command
C. Configure the snmp ifindex persist command on the physical interfaces.
D. Trigger a new snmpwalk from the monitoring system to synchronize interface OIDs
Answer: A

377.Refer to the exhibit.

```
R2#show policy-map control-plane
 Control Plane
  Service-policy input: CoPP
    Class-map: SSH (match-all)
      29 packets, 2215 bytes
      5 minute offered rate 0000 bps
      Match: access-group 100

    Class-map: ANY (match-all)
      46 packets, 3878 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group 199
      drop

    Class-map: class-default (match-any)
      41 packets, 5687 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any

R2#show access-list 100
Extended IP access list 100
    10 deny tcp any any eq 22 (14 matches)
    20 permit tcp host 192.168.12.1 any eq 22 (29 matches)
R2#show access-list 199
Extended IP access list 199
    10 permit ip any any (51 matches)
```

Which action limits the access to R2 from 192.168.12.1?

A. Swap sequence 10 with sequence 20 in access-list 100.

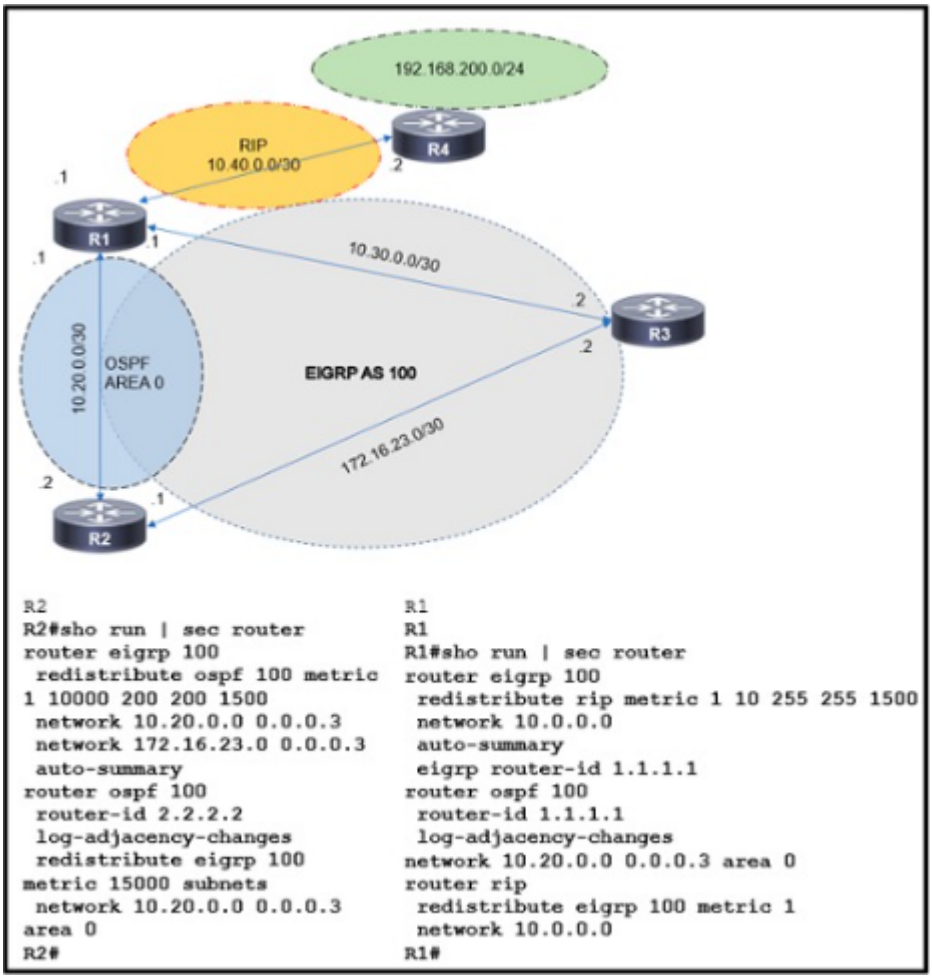
B. Modify sequence 20 to permit tcp host 192.168.12.1 eq 22 any to access-list 100

C. Swap sequence 20 with sequence 10 in access-list 100

D. Modify sequence 10 to deny tcp any eq 22 any to access-list 100.

Answer: C

378.Refer to the exhibit




```
R2                                  R1
R2#sho run | sec router             R1
router eigrp 100                    R1#sho run | sec router
 redistribute ospf 100 metric       router eigrp 100
1 10000 200 200 1500                 redistribute rip metric 1 10 255 255 1500
 network 10.20.0.0 0.0.0.3           network 10.0.0.0
 network 172.16.23.0 0.0.0.3         auto-summary
 auto-summary                        eigrp router-id 1.1.1.1
router ospf 100                     router ospf 100
 router-id 2.2.2.2                   router-id 1.1.1.1
 log-adjacency-changes               log-adjacency-changes
 redistribute eigrp 100             network 10.20.0.0 0.0.0.3 area 0
metric 15000 subnets                router rip
 network 10.20.0.0 0.0.0.3           redistribute eigrp 100 metric 1
area 0                               network 10.0.0.0
R2#                                 R1#
```

The route to 192 168 200 0 is flapping between R1 and R2.
Which set of configuration changes resolves the flapping route?

- R2(config)#**router ospf 100**
  R2(config-router)#**no redistribute eigrp 100**
  R2(config-router)#**redistribute eigrp 100 metric 1 subnets**

- R1(config)#**no router rip**
  R1(config)#**ip route 192.168.200.0 255.255.255.0 10.40.0.2**

- R2(config)#**router eigrp 100**
  R2(config-router)#**no redistribute ospf 100**
  R2(config-router)#**redistribute rip**

- R1(config)#**router ospf 100**
  R1(config-router)#**redistribute rip metric 1 metric-type 1 subnets**

A. Option A
B. Option B
C. Option C
D. Option D
Answer: D

379.Refer to the exhibit.

```
R1 (config)# ip vrf CCNP
R1 (config-vrf)# rd 1:100
R1 (config-vrf)# exit
R1 (config)# interface Loopback0
R1 (config-if)# ip address 10.1.1.1 255.255.255.0
R1 (config-if)# ip vrf forwarding CCNP
R1 (config-if)# exit
R1 (config)# exit
R1# ping vrf CCNP 10.1.1.1
% Unrecognized host or address, or protocol not running.
```

Which command must be configured to make VRF CCNP work?

```
interface Loopback0
 ip address 10.1.1.1 255.255.255.0
 vrf forwarding CCNP

interface Loopback0
 ip address 10.1.1.1 255.255.255.0

interface Loopback0
 vrf forwarding CCNP

interface Loopback0
 ip address 10.1.1.1 255.255.255.0
 ip vrf forwarding CCNP
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: B

380.Refer to the exhibit.

```
ip sla 1
 icmp-echo 8.8.8.8
 threshold 1000
 timeout 2000
 frequency 5
ip sla schedule 1 life forever start-time now
!
track 1 ip sla 1
!
ip route 0.0.0.0 0.0.0.0 Ethernet0/0 203.0.113.1 name ISP1 track
1
ip route 0.0.0.0 0.0.0.0 Ethernet0/1 198.51.100.1 2 name ISP2
```

After recovering from a power failure. Ethernet0/1 stayed down while Ethernet0/0 returned to the up/up state. The default route through ISP1 was not reinstated m the routing table until Ethernet0/1 also came up.

Which action resolves the issue?

A. Reference the track object 1 in both static default routes

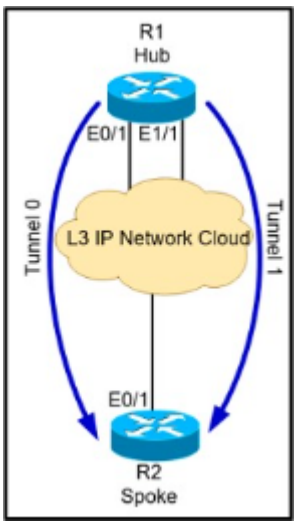
B. Remove the references to the interface names from both static default routes

C. Configure the default route through ISP1 with a higher administrative distance than 2.

D. Add a static route to the 8 8.8 8/32 destination through the next hop 203.0.113.1

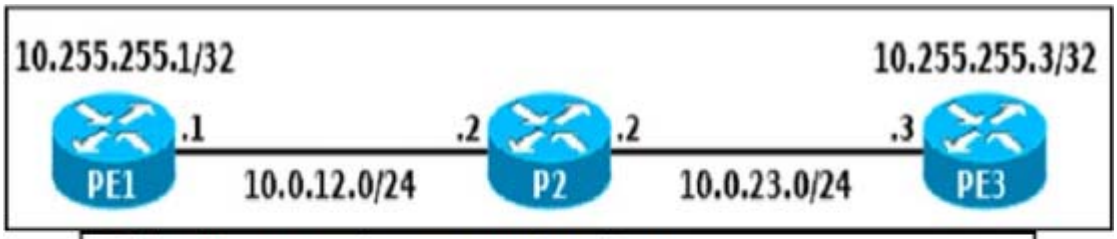
Answer: A

381.Refer to me exhibit.



The hub and spoke are connected via two DMVPN tunnel interfaces The NHRP is configured and the tunnels are detected on the hub and the spoke.
Which configuration command adds an IPsec profile on both tunnel interfaces to encrypt traffic?
A. tunnel protection ipsec profile DMVPN multipoint
B. tunnel protection ipsec profile DMVPN tunnel1
C. tunnel protection ipsec profile DMVPN shared
D. tunnel protection ipsec profile DMVPN unique
Answer: C

382.Refer to the exhibit.




```
PE1# show run | sec router bgp
router bgp 65000
 bgp log-neighbor-changes
 neighbor 10.255.255.3 remote-as 65000
 neighbor 10.255.255.3 update-source Loopback0
1/1/1 ms
```

```
PE1# debug ip tcp transactions
PE1# debug ip icmp

[...snip...]
*Feb 22 14:04:12.374: TCP: sending SYN, seq 379810712, ack 0
*Feb 22 14:04:12.374: TCP0: Connection to 10.255.255.3:179,
advertising MSS 1460
*Feb 22 14:04:12.374: TCP0: state was CLOSED -> SYNSENT [21381 -
> 10.255.255.3(179)]
*Feb 22 14:04:12.375: ICMP: dst (10.255.255.1) administratively
prohibited unreachable rcv from 10.0.12.2
*Feb 22 14:04:12.375: TCP0: ICMP destination unreachable
received
*Feb 22 14:04:12.375: Released port 21381 in Transport Port
Agent for TCP IP type 1 delay 240000
*Feb 22 14:04:12.375: TCP0: state was SYNSENT -> CLOSED [21381 -
> 10.255.255.3(179)]
*Feb 22 14:04:12.375: TCB 0xE35A92B8 destroyed
```

The administrator is troubleshooting a BGP peering between PE1 and PE3 that is unable to establish. Which action resolves the issue?

A. P2 must have a route to PE3 to establish a BGP session to PE1

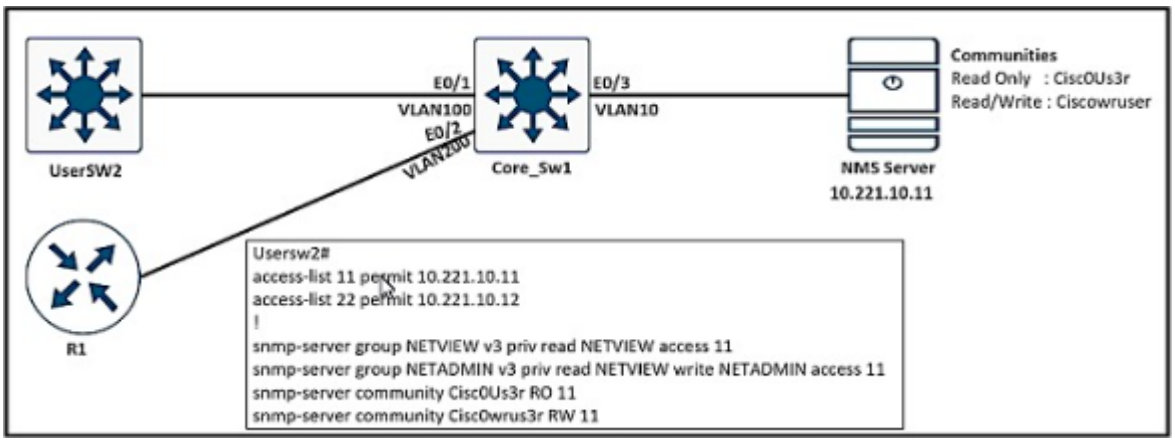
B. Disable sending ICMP unreachables on P2 to allow PE1 to establish a session with PE3

C. Ensure that the PE3 loopback address is used as a source for BGP peering to PE1

D. Remove the traffic filtering rules on P2 blocking the BGP communication between PE1 and PE3

Answer: C

383.Refer to the exhibit.



An engineer configured SNMP Commîmes on UserSW2 switch, but the SNMP server cannot upload modified configurations to the switch.

Which configuration resolves this issue?

A. snmp-server community Ciscowruser RW 11

B. snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22

C. snmp-server community CiscOUs3r RW 11

D. snmp-server group NETVIEW v2c priv read NETVIEW access 11

Answer: A

384.Refer to the exhibit.

```
R1#sh run | section eigrp
router eigrp 10
network 10.10.10.0 0.0.0.255
no auto-summary
neighbor 10.10.10.2 FastEthernet0/0
neighbor 10.10.10.3 FastEthernet0/0

R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address                 Interface       Hold Uptime   SRTT   RTO    Q
Seq                                         (sec)         (ms)       Cnt
Num
1   10.10.10.2              Fa0/0             10 00:01:01   42   232  0  6
0   10.10.10.3              Fa0/0             10 00:01:03   43   244  0  6
```

The remote branch locations have a static neighbor relationship configured to R1 only R1 has successful neighbor relationships with the remote locations of R2 and R3, but the end users cannot communicate with each other.

Which configuration resolves the issue'

R2
```
interface FastEthernet0/0.10
 encapsulation dot1Q
 ip address 10.10.10.2 255.255.255.0
```

R3
```
interface FastEthernet0/0.10
 encapsulation dot1Q
 ip address 10.10.10.3 255.255.255.0
```

R2
interface FastEthernet0/0.10
encapsulation dot1Q
ip address 10.10.10.2 255.255.255.0

R3
interface FastEthernet0/0.10
encapsulation dot1Q
ip address 10.10.10.3 255.255.255.0

R2
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 10.10.10.2 255.255.255.0

R3
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 10.10.10.3 255.255.255.0

R2 and R3
interface FastEthernet0/0
no ip split-horizon eigrp 10

R1
interface FastEthernet0/0
no ip split-horizon eigrp 10

A. Option A
B. Option B
C. Option C
D. Option D
E. Option E
Answer: E

385.Refer to the exhibit.

```
enable secret 5 <password>
username cisco privilege 15 secret 5 <password>
username operator password 7 <password>
line vty 0 4
session-timeout 240
password 7 <password>
transport input telnet
```

The authentication is not working as desired and the user drops into user-exec mode.
Which configuration resolves the issue?

aaa new-model
aaa authentication login default local
aaa authorization exec default local
!
line vty 0 4
login authentication default
authorization exec default

aaa new-model
aaa authentication login default local
aaa authorization priv default 15
!
line vty 0 4
login authentication default
authorization exec priv15

```
aaa new-model
 aaa authentication login local
 aaa authorization exec local
 !
 line vty 0 4
  login authentication local
  authorization exec default
```

```
aaa new-model
 aaa authentication common-id default local
 aaa authorization exec default local
 !
 line vty 0 4
  login authentication default
  authorization exec default
```

A. Option A

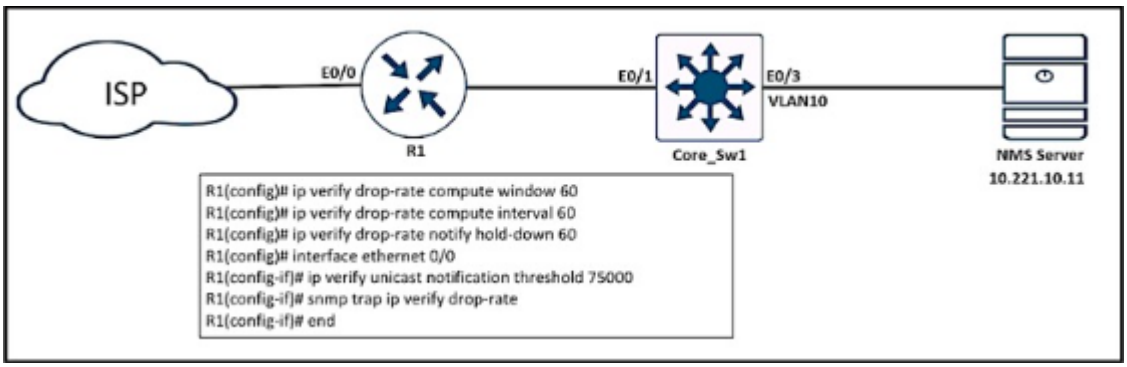
B. Option B

C. Option C

D. Option D

Answer: C

386.Refer to the exhibit.



An engineer configured SNMP traps to record spoofed packets drop of more than 48000 a minute on the ethernet0/0 interlace. During an IP spoofing attack, the engineer noticed that no notifications have been received by the SNMP server.

Which configuration resolves the issue on R1?

A. ip verity unicast notification threshold 48000

B. ip verify unicast notification threshold 8000

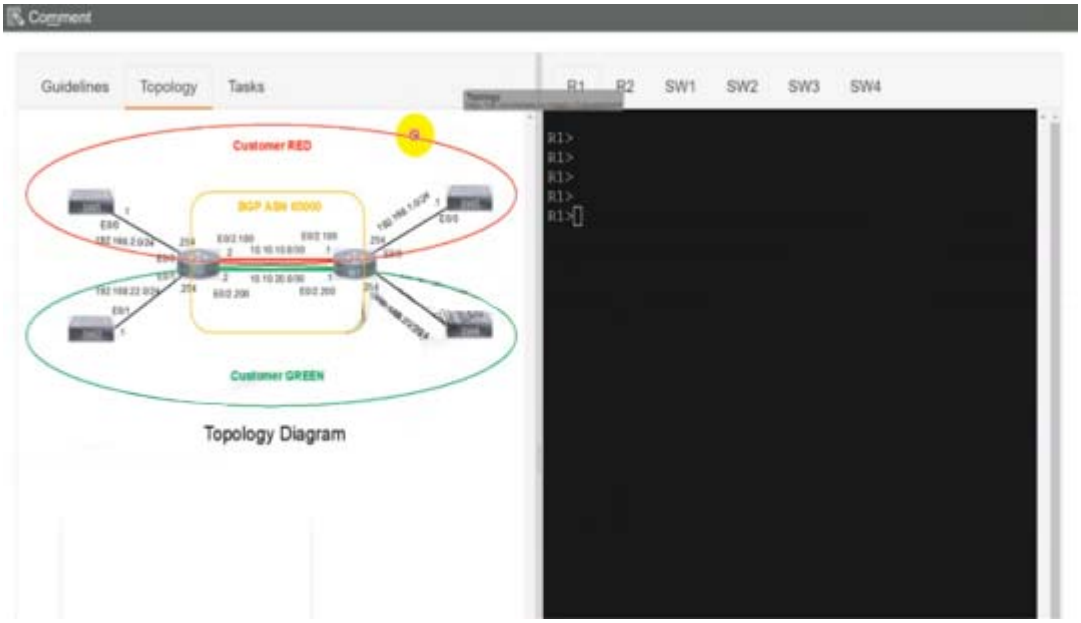
C. ip verify unicast notification threshold 800

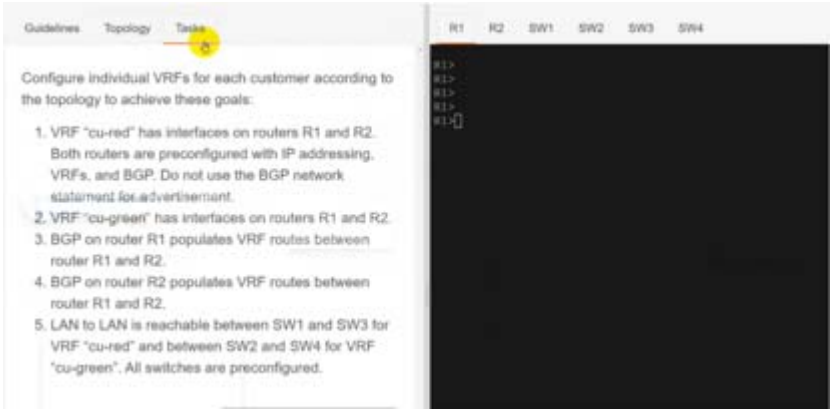
D. ip verify unicast notification threshold 80

Answer: C

387.LAB SIMULATION

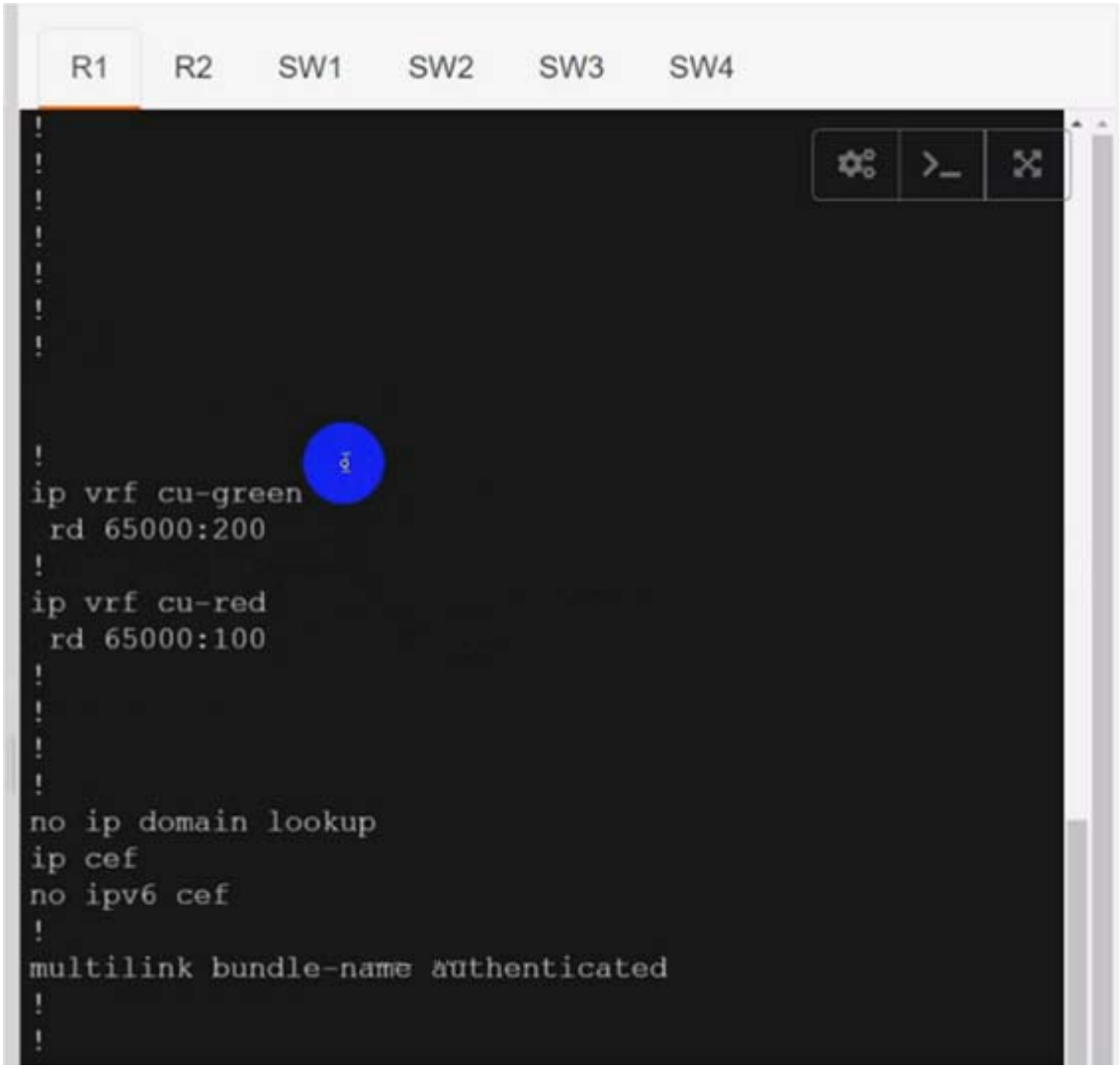
Configure individual VRFs for each customer according to the topology to achieve these goals:

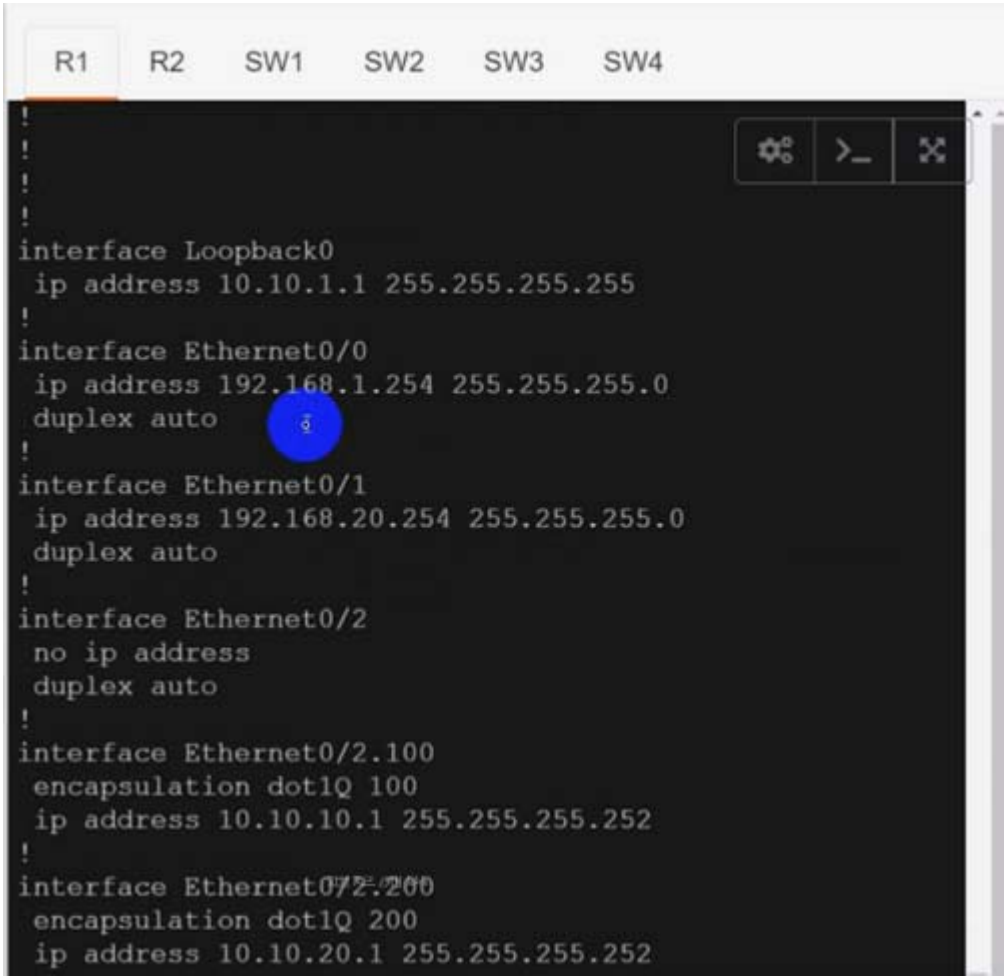

Comment
Guidelines
Topology
Tasks
R1
R2
SW1
SW2
SW3
SW4
Customer RED
Customer GREEN
Topology Diagram
R1>
R1>
R1>
R1>
R1>

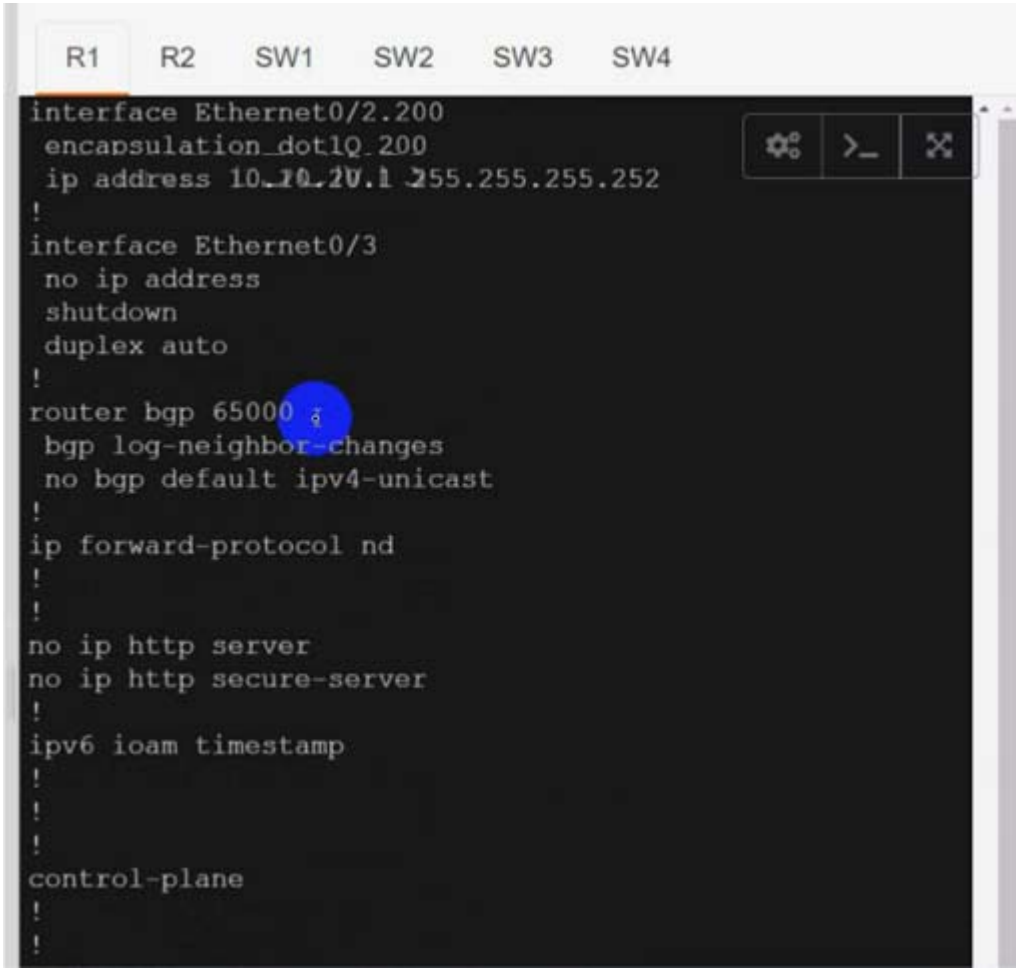

Guidelines
Topology
Tasks
Configure individual VRFs for each customer according to the topology to achieve these goals:
1. VRF "cu-red" has interfaces on routers R1 and R2. Both routers are preconfigured with IP addressing, VRFs, and BGP. Do not use the BGP network statement for advertisement.
2. VRF "cu-green" has interfaces on routers R1 and R2.
3. BGP on router R1 populates VRF routes between router R1 and R2.
4. BGP on router R2 populates VRF routes between router R1 and R2.
5. LAN to LAN is reachable between SW1 and SW3 for VRF "cu-red" and between SW2 and SW4 for VRF "cu-green". All switches are preconfigured.
R1
R2
SW1
SW2
SW3
SW4
R1>
R1>
R1>
R1>
R1>

R1

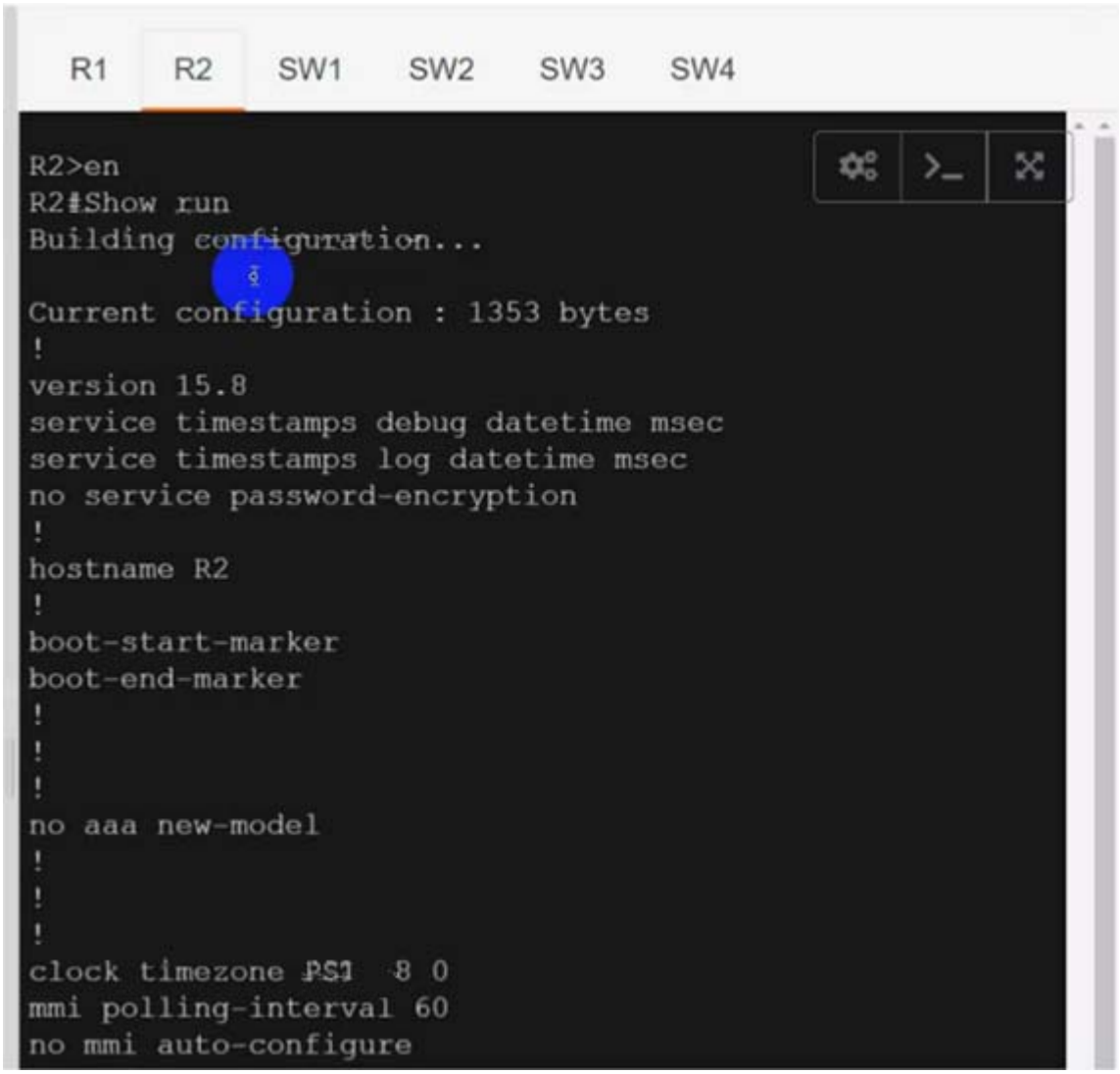

R1
R2
SW1
SW2
SW3
SW4
CHINESEDUMPS
通过测试
R1>
R1>
R1>
R1>
R1>en
R1#sh run
Building configuration...
Current configuration : 1353 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!


R1
R2
SW1
SW2
SW3
SW4
!
!
!
!
!
!
!
!
ip vrf cu-green
rd 65000:200
!
ip vrf cu-red
rd 65000:100
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!

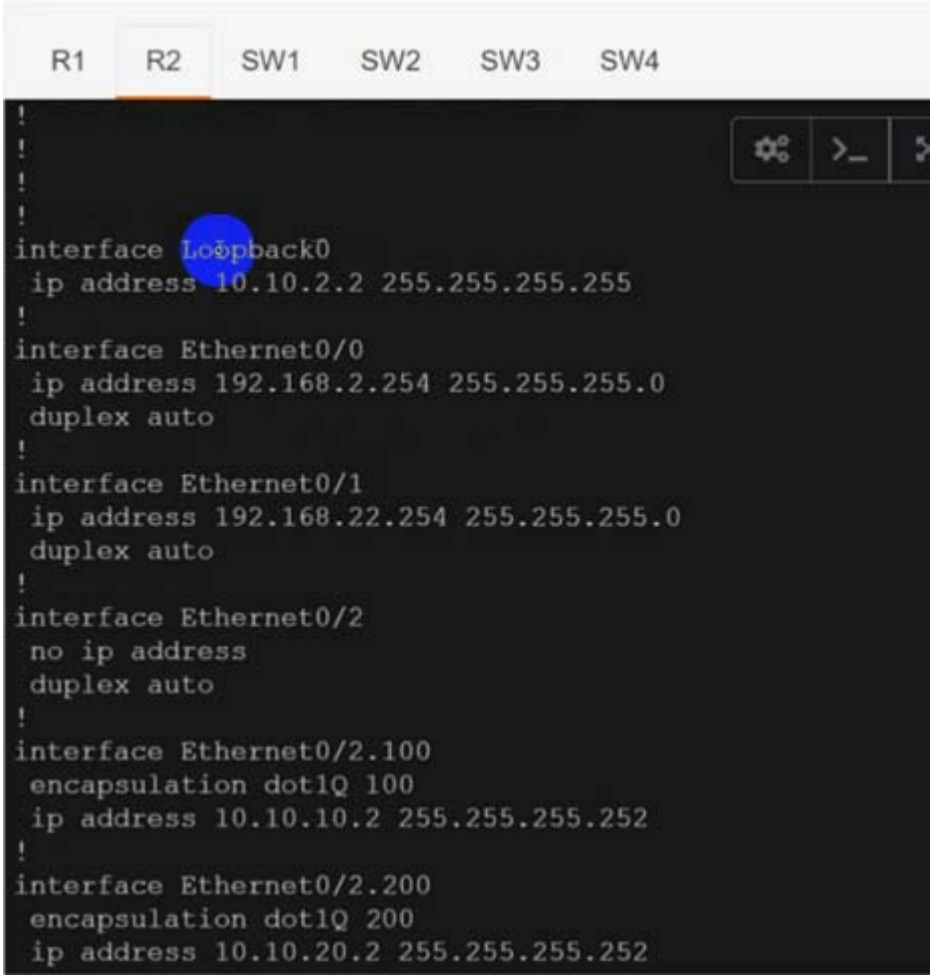

R1
R2
SW1
SW2
SW3
SW4
!
!
!
!
interface Loopback0
ip address 10.10.1.1 255.255.255.255
!
interface Ethernet0/0
ip address 192.168.1.254 255.255.255.0
duplex auto
!
interface Ethernet0/1
ip address 192.168.20.254 255.255.255.0
duplex auto
!
interface Ethernet0/2
no ip address
duplex auto
!
interface Ethernet0/2.100
encapsulation dot1Q 100
ip address 10.10.10.1 255.255.255.252
!
interface Ethernet0/2.200
encapsulation dot1Q 200
ip address 10.10.20.1 255.255.255.252

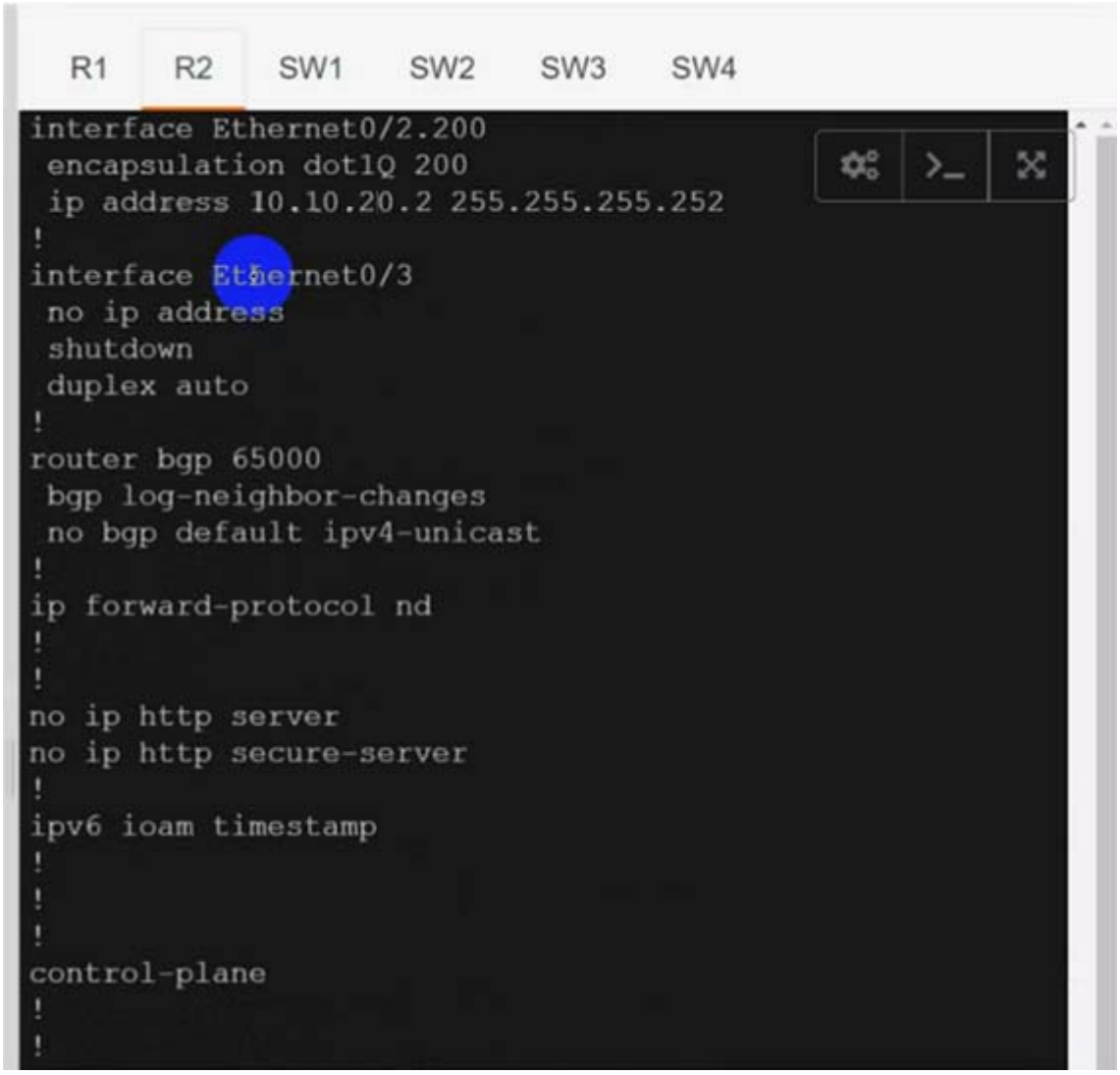

R1
R2
SW1
SW2
SW3
SW4
interface Ethernet0/2.200
encapsulation dot1Q 200
ip address 10.10.20.1 255.255.255.252
!
interface Ethernet0/3
no ip address
shutdown
duplex auto
!
router bgp 65000
bgp log-neighbor-changes
no bgp default ipv4-unicast
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
!
!
control-plane
!
!

R2

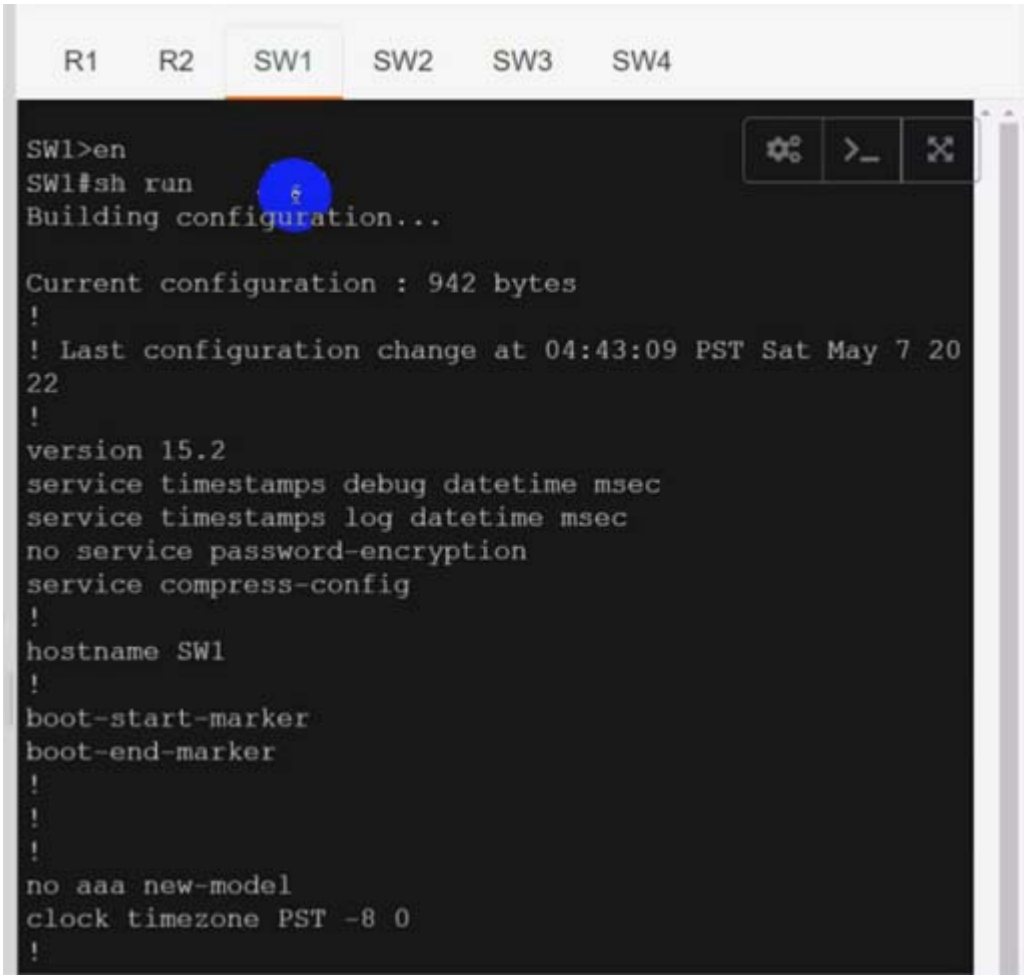

R1
R2
SW1
SW2
SW3
SW4
R2>en
R2#Show run
Building configuration...
Current configuration : 1353 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
clock timezone PST 8 0
mmi polling-interval 60
no mmi auto-configure

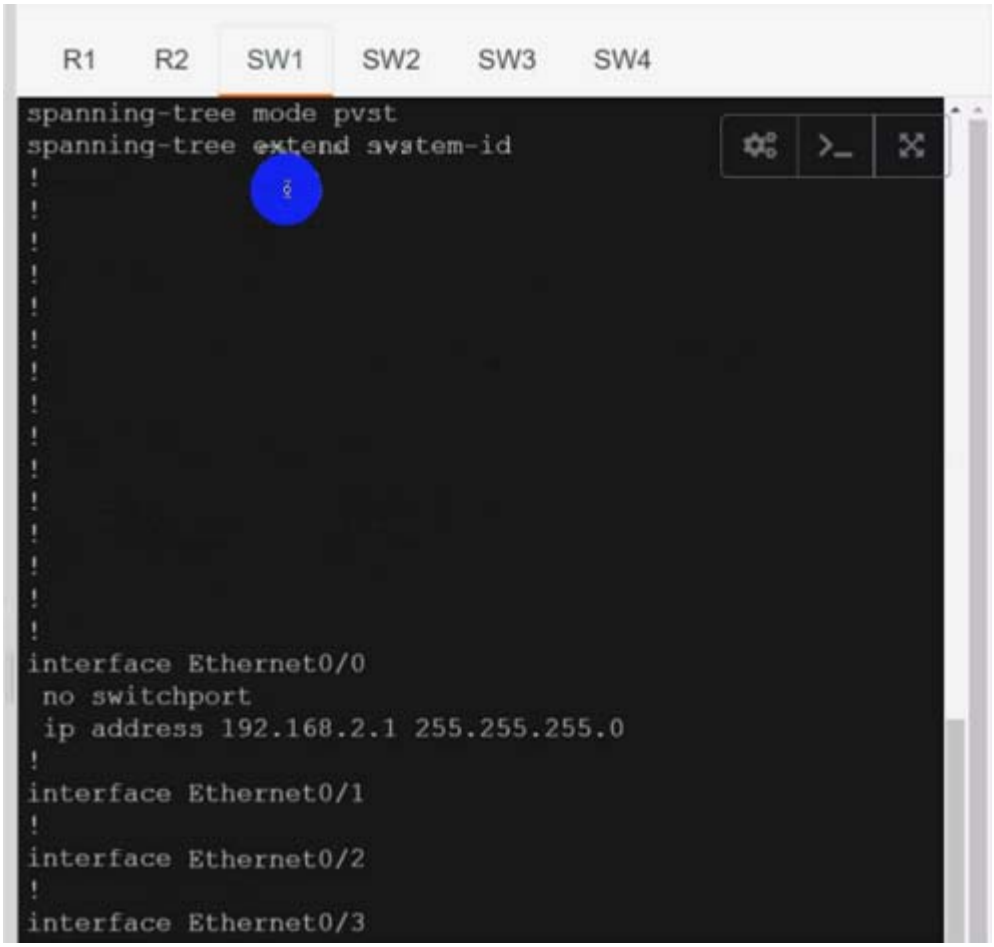

R1
R2
SW1
SW2
SW3
SW4
!
!
!
!
!
!
!
!
ip vrf cu-green
rd 65000:200
!
ip vrf cu-red
rd 65000:100
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!

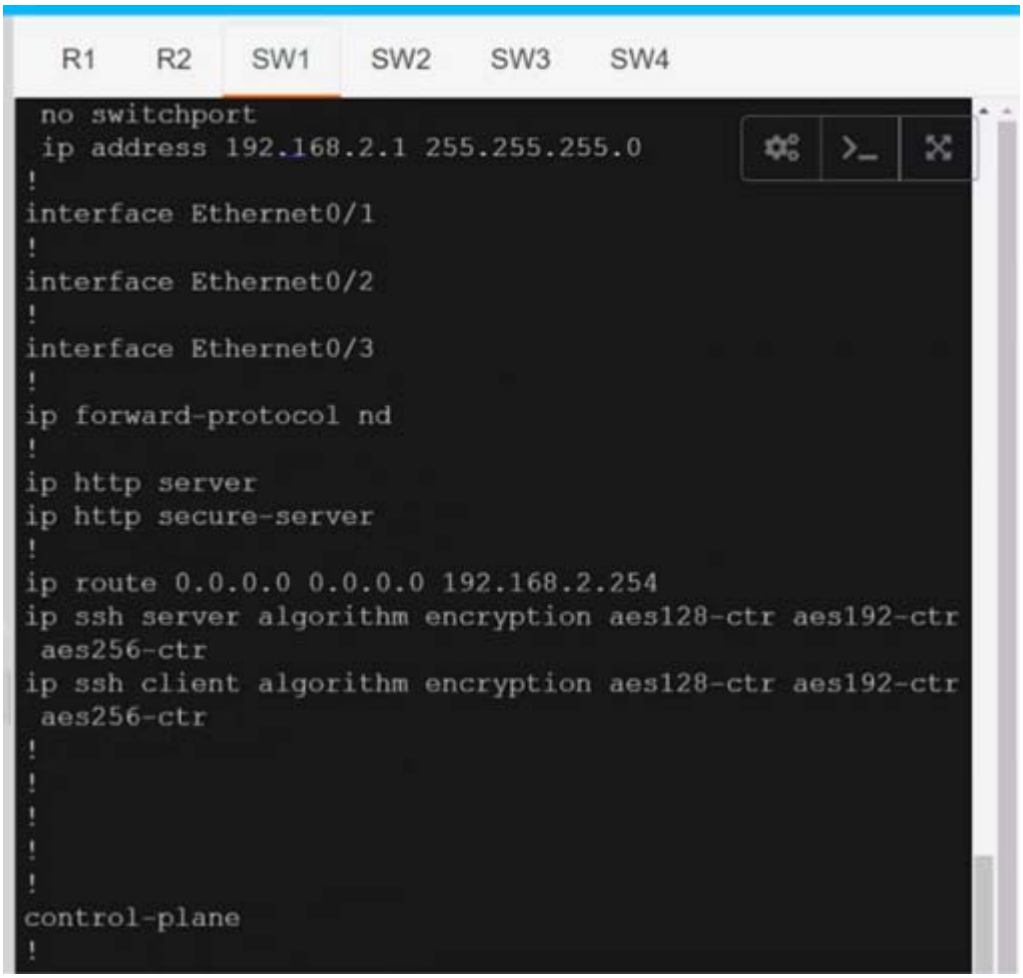

R1
R2
SW1
SW2
SW3
SW4
!
!
!
!
interface Loopback0
ip address 10.10.2.2 255.255.255.255
!
interface Ethernet0/0
ip address 192.168.2.254 255.255.255.0
duplex auto
!
interface Ethernet0/1
ip address 192.168.22.254 255.255.255.0
duplex auto
!
interface Ethernet0/2
no ip address
duplex auto
!
interface Ethernet0/2.100
encapsulation dot1Q 100
ip address 10.10.10.2 255.255.255.252
!
interface Ethernet0/2.200
encapsulation dot1Q 200
ip address 10.10.20.2 255.255.255.252


R1
R2
SW1
SW2
SW3
SW4
interface Ethernet0/2.200
encapsulation dot1Q 200
ip address 10.10.20.2 255.255.255.252
!
interface Ethernet0/3
no ip address
shutdown
duplex auto
!
router bgp 65000
bgp log-neighbor-changes
no bgp default ipv4-unicast
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
!
!
control-plane
!
!

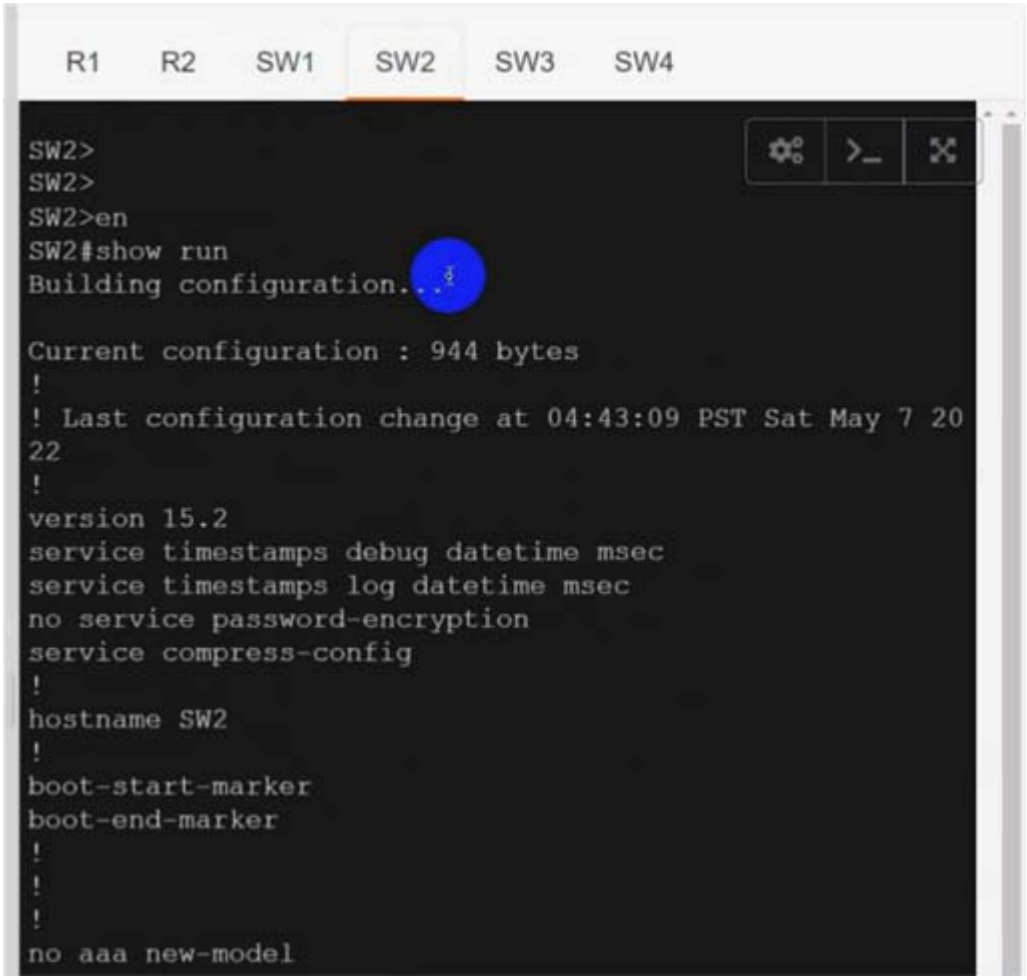
SW1

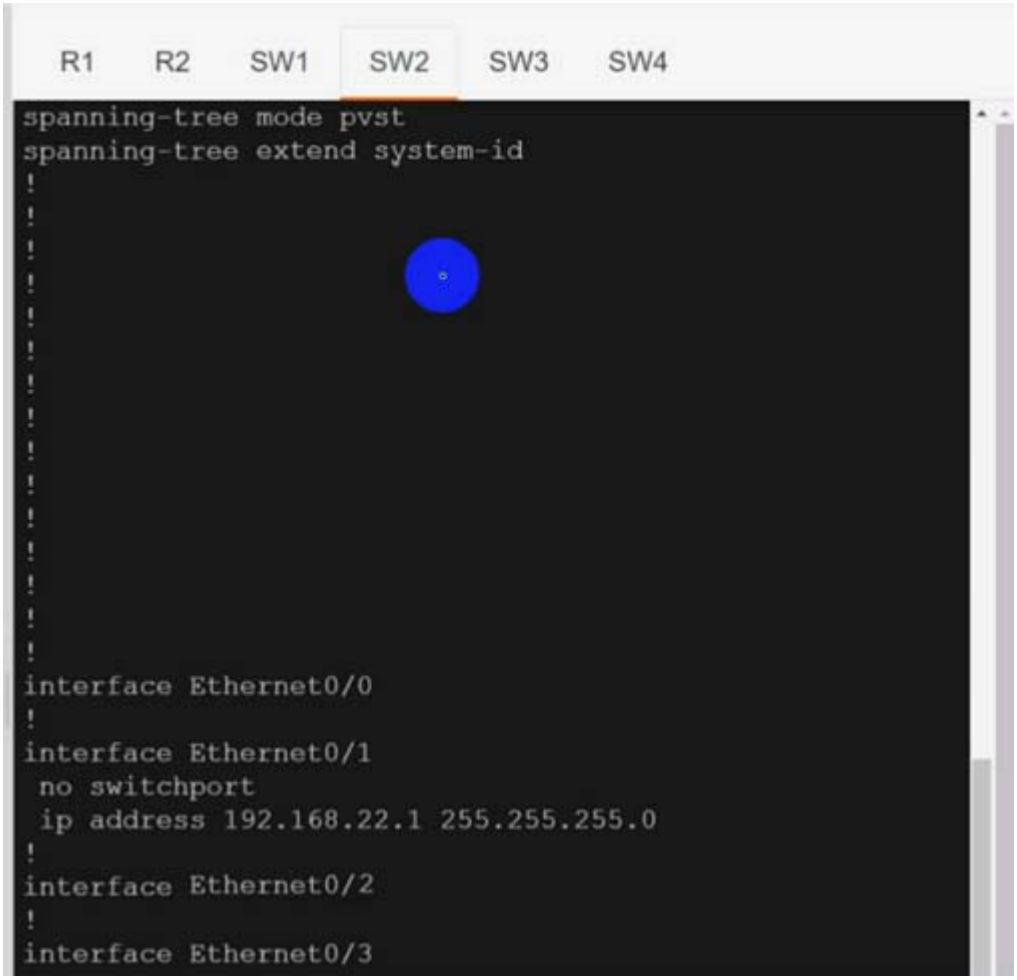

R1
R2
SW1
SW2
SW3
SW4
SW1>en
SW1#sh run
Building configuration...
Current configuration : 942 bytes
!
! Last configuration change at 04:43:09 PST Sat May 7 20
22
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
!

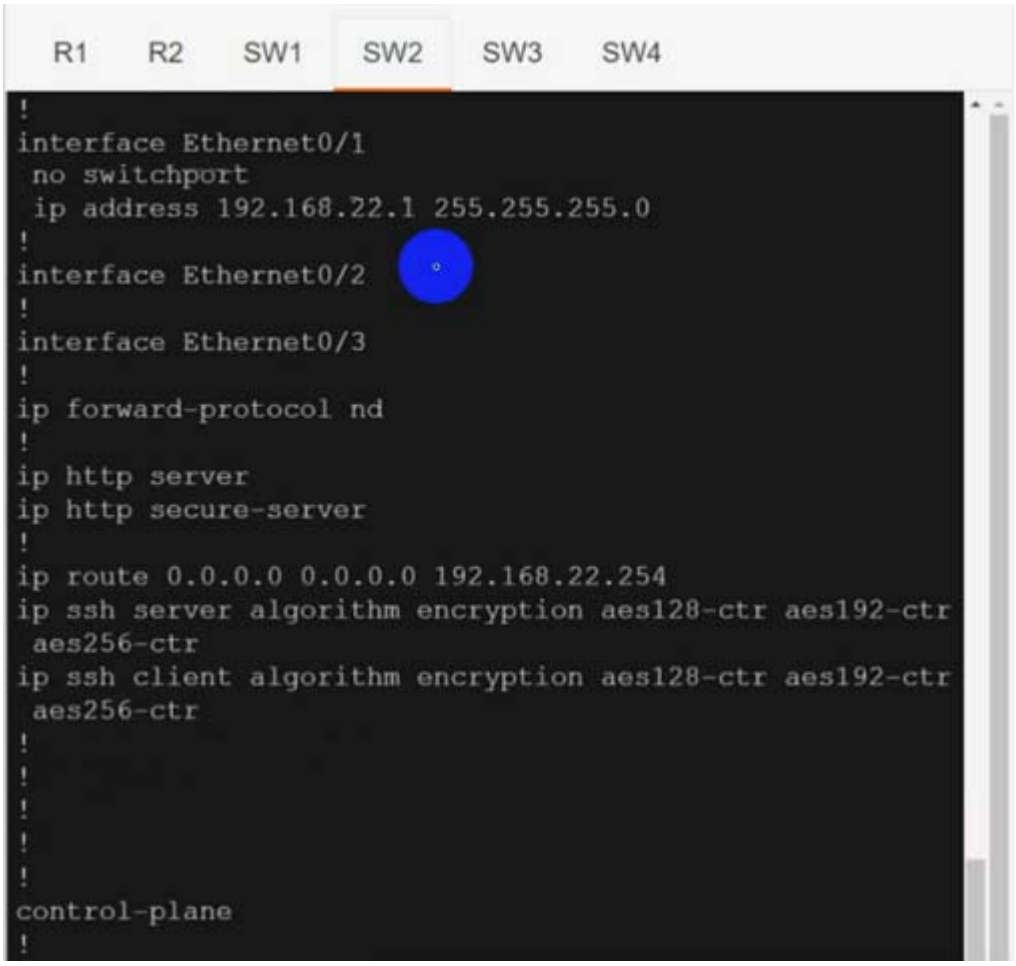

R1
R2
SW1
SW2
SW3
SW4
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
no switchport
ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3


R1
R2
SW1
SW2
SW3
SW4
no switchport
ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.2.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
!
!
!
!
!
control-plane
!

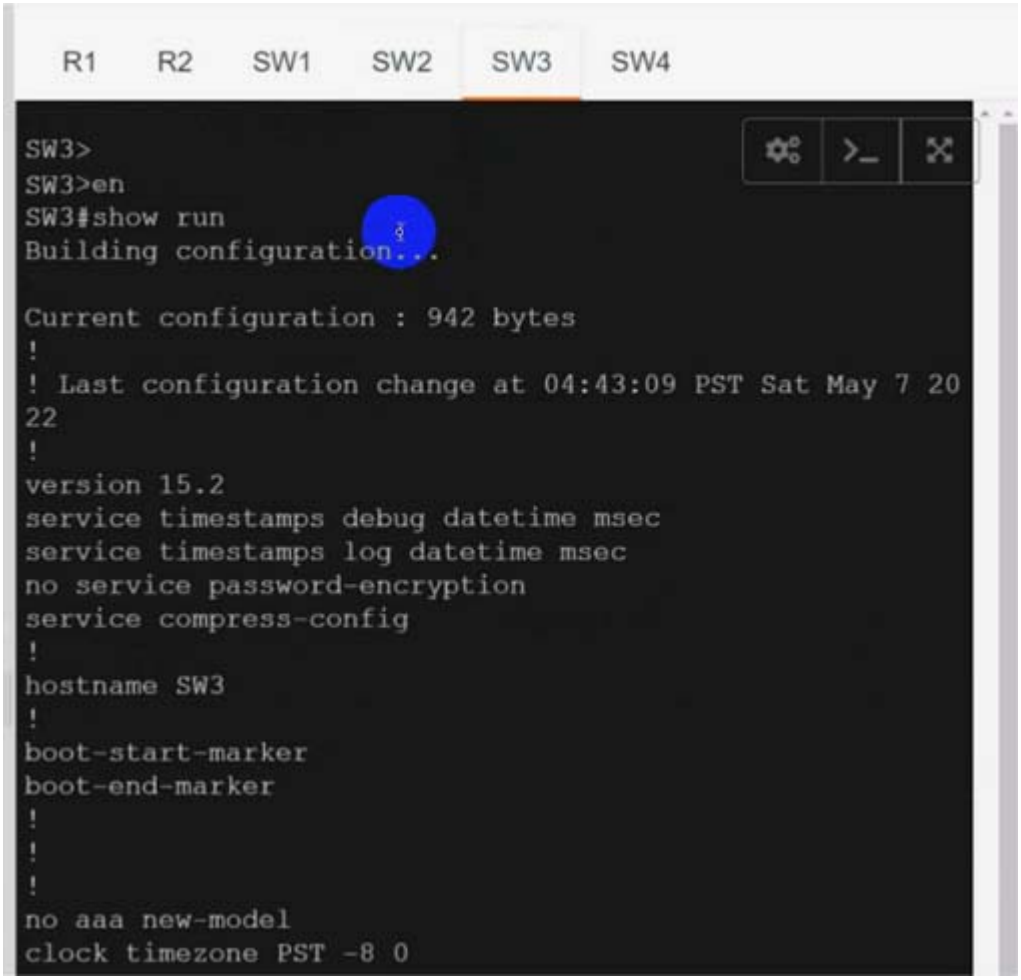
SW2

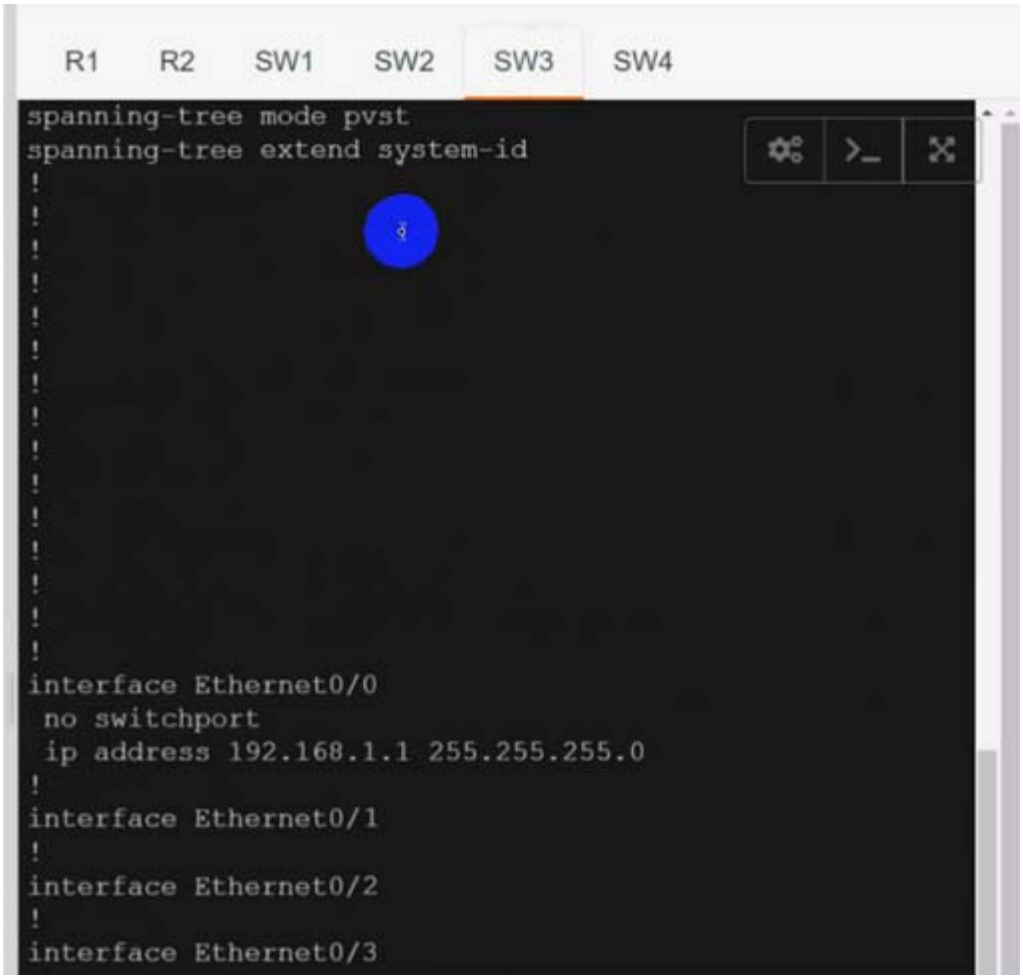

R1
R2
SW1
SW2
SW3
SW4
SW2>
SW2>
SW2>en
SW2#show run
Building configuration...
Current configuration : 944 bytes
!
! Last configuration change at 04:43:09 PST Sat May 7 20
22
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model

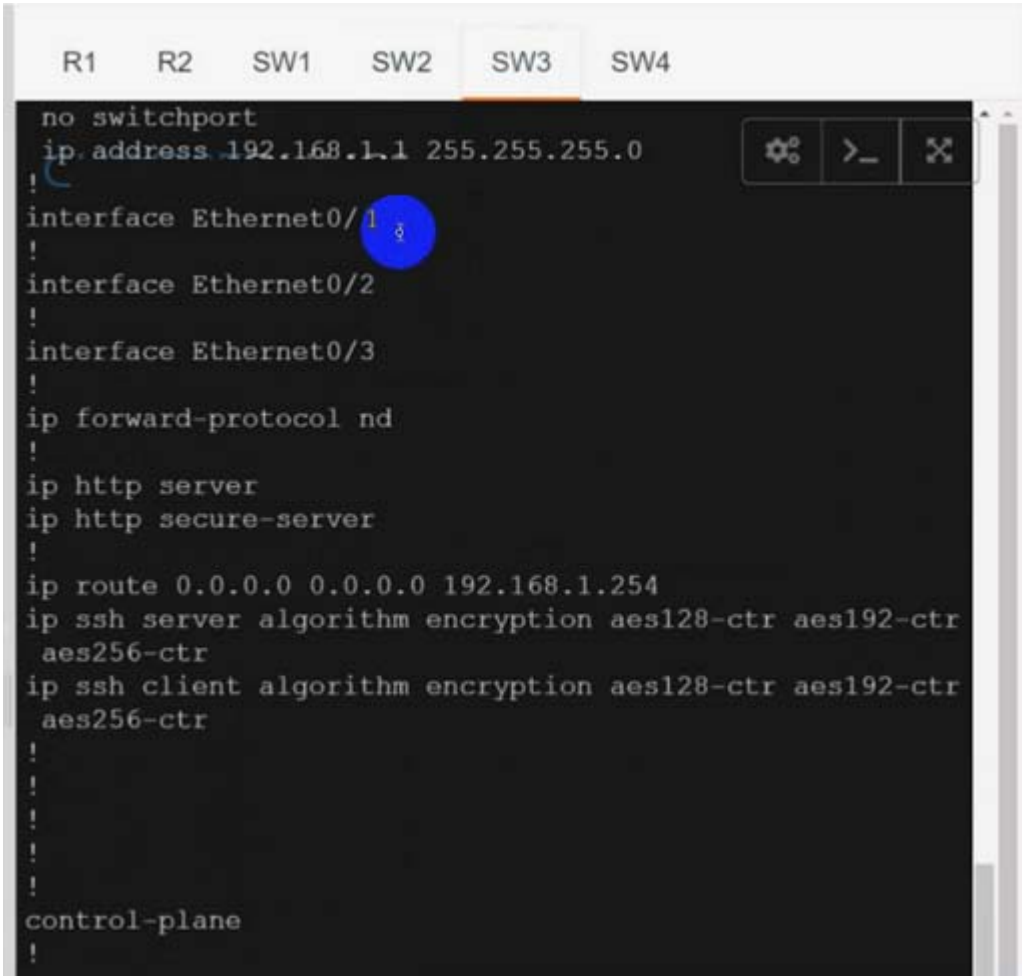

R1
R2
SW1
SW2
SW3
SW4
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
!
interface Ethernet0/1
no switchport
ip address 192.168.22.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3

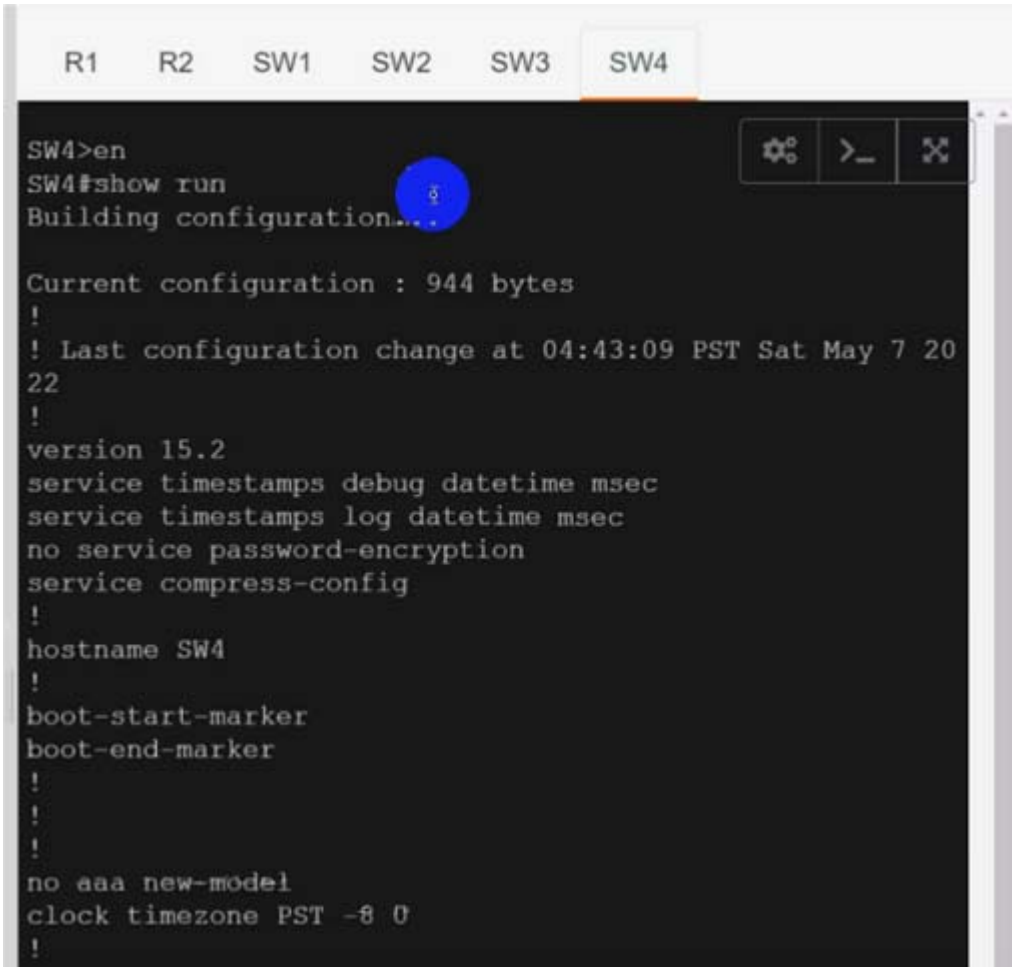

R1
R2
SW1
SW2
SW3
SW4
!
interface Ethernet0/1
no switchport
ip address 192.168.22.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.22.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
!
!
!
!
!
control-plane
!

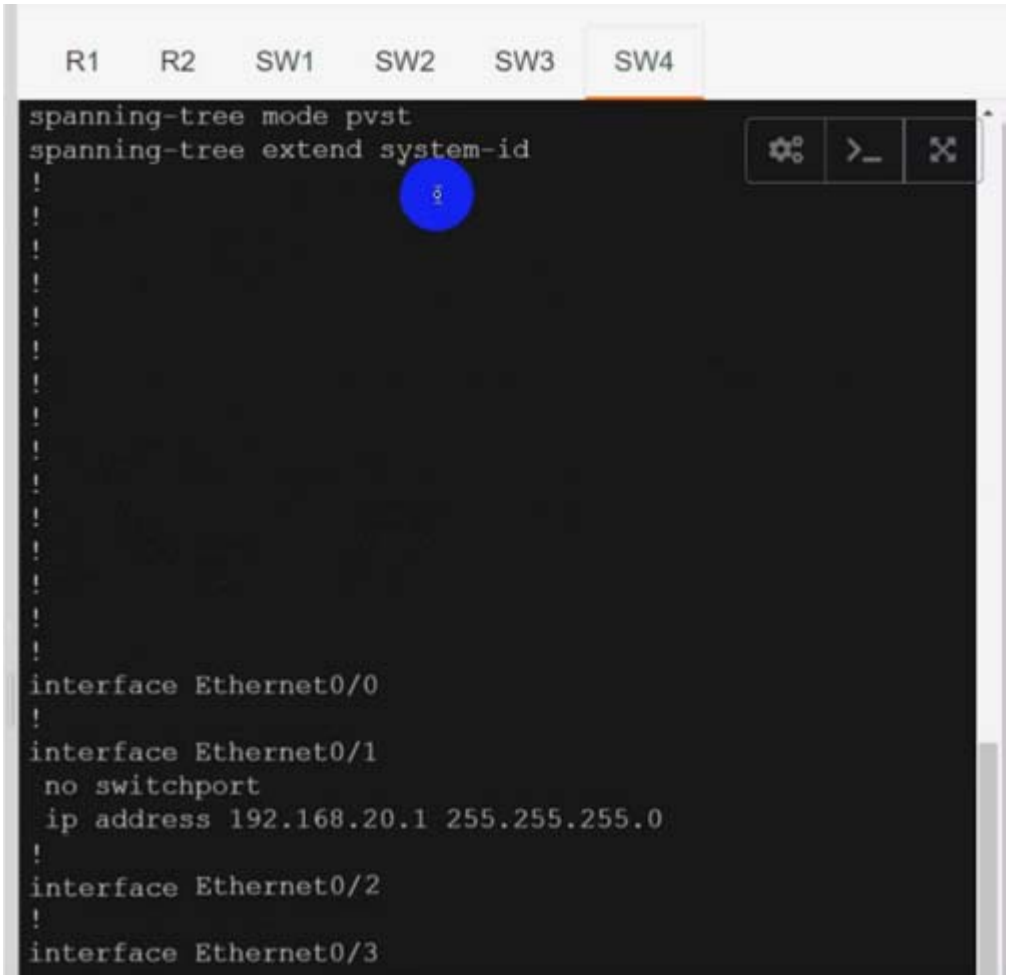
SW3

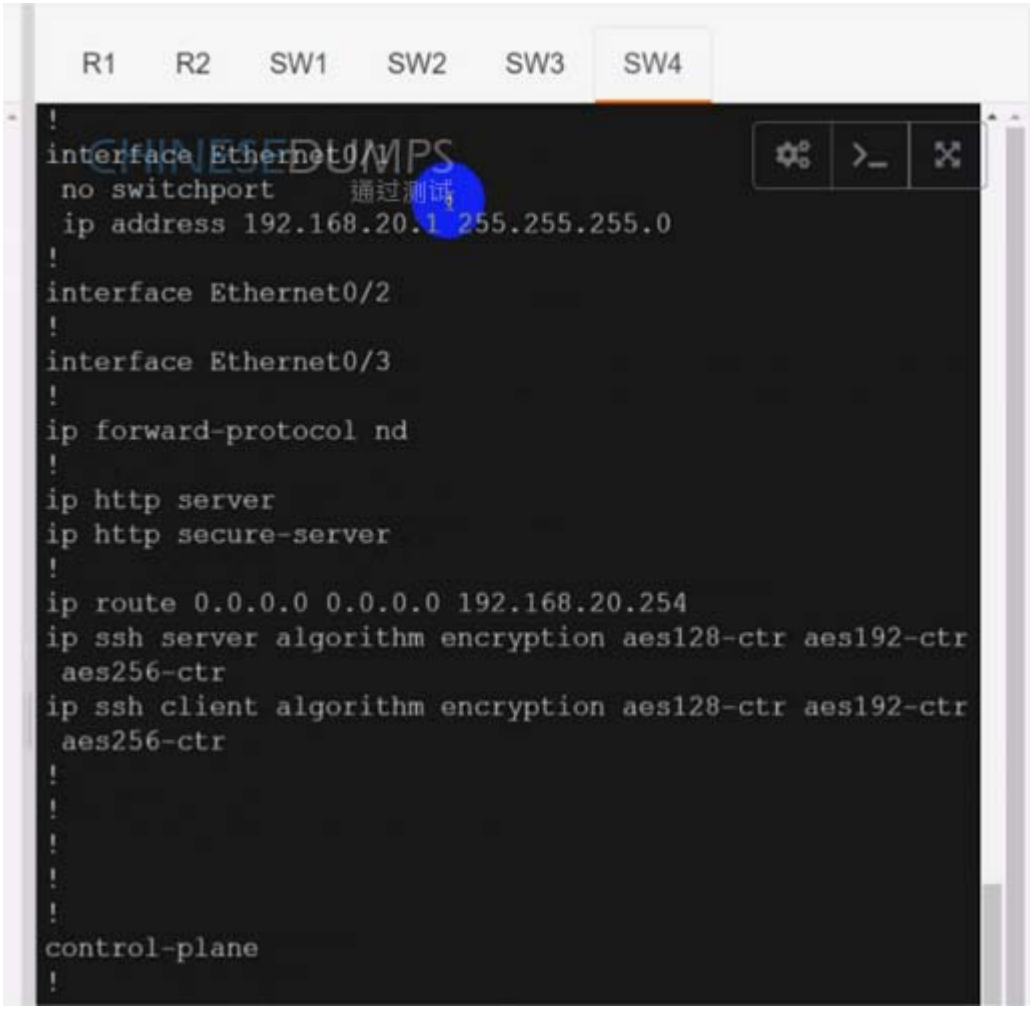

R1
R2
SW1
SW2
SW3
SW4
SW3>
SW3>en
SW3#show run
Building configuration...
Current configuration : 942 bytes
!
! Last configuration change at 04:43:09 PST Sat May 7 20
22
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW3
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0

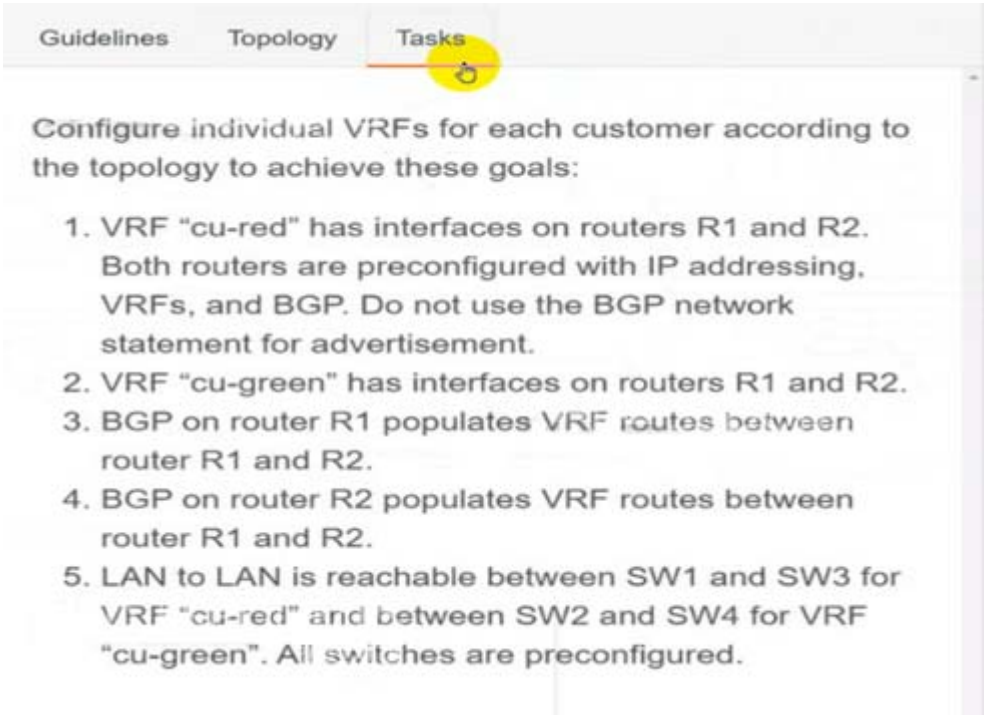

R1
R2
SW1
SW2
SW3
SW4
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
no switchport
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3


R1
R2
SW1
SW2
SW3
SW4
no switchport
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
!
!
!
!
!
control-plane
!


R1
R2
SW1
SW2
SW3
SW4
SW4>en
SW4#show run
Building configuration...
Current configuration : 944 bytes
!
! Last configuration change at 04:43:09 PST Sat May 7 20
22
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW4
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone PST -8 0
!


R1
R2
SW1
SW2
SW3
SW4
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
!
interface Ethernet0/1
no switchport
ip address 192.168.20.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3


R1
R2
SW1
SW2
SW3
SW4
!
interface Ethernet0/1
no switchport
ip address 192.168.20.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.20.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
!
!
!
!
!
control-plane
!


Guidelines
Topology
Tasks
Configure individual VRFs for each customer according to the topology to achieve these goals:
1. VRF "cu-red" has interfaces on routers R1 and R2. Both routers are preconfigured with IP addressing, VRFs, and BGP. Do not use the BGP network statement for advertisement.
2. VRF "cu-green" has interfaces on routers R1 and R2.
3. BGP on router R1 populates VRF routes between router R1 and R2.
4. BGP on router R2 populates VRF routes between router R1 and R2.
5. LAN to LAN is reachable between SW1 and SW3 for VRF "cu-red" and between SW2 and SW4 for VRF "cu-green". All switches are preconfigured.

Answer:

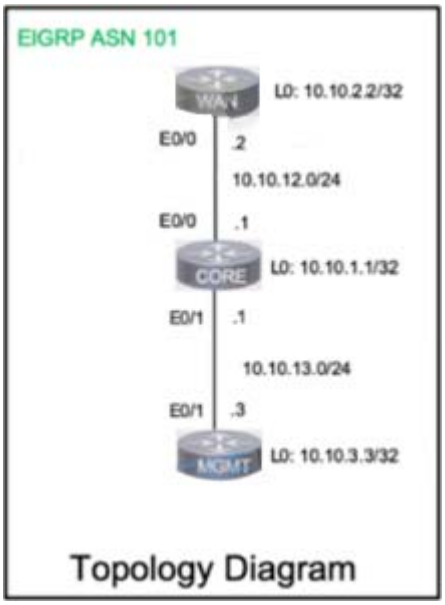
Solution:
1) Use cu-red under interfaces facing SW1 & SW3:
On R1:
interface Ethernet0/0
ip vrf forwarding cu-red
ip address 192.168.1.254 255.255.255.0
Check reachability to SW1:
R1#ping vrf cu-red 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
On R2:
interface Ethernet0/0
ip vrf forwarding cu-red
ip address 192.168.2.254 255.255.255.0
Check reachability to SW3:
R2#ping vrf cu-red 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
2) Use vrf cu-green for SW2 & SW4:
On R1:
interface Ethernet0/1
ip vrf forwarding cu-green
ip address 192.168.20.254 255.255.255.0
Test reachability to SW2:
R1#ping vrf cu-green 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.22.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
On R2:
interface Ethernet0/1
ip vrf forwarding cu-green
ip address 192.168.22.254 255.255.255.0
Test reachability to SW4:
R2#ping vrf cu-green 192.168.22.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
3) On R1:
interface Ethernet0/2.100

mpls ip
!
interface Ethernet0/2.200
mpls ip
!
Configure BGP:
router bgp 65000
neighbor 10.10.10.2 remote-as 65000
neighbor 10.10.20.2 remote-as 65000
!
address-family vpnv4
neighbor 10.10.10.2 activate
neighbor 10.10.20.2 activate
exit-address-family
!
address-family ipv4 vrf cu-green
redistribute connected
exit-address-family
!
address-family ipv4 vrf cu-red
redistribute connected
exit-address-family
!
R1(config)#ip vrf cu-red
R1(config-vrf)#route-target both 65000:100
!
R1(config)#ip vrf cu-green
R1(config-vrf)#route-target both 65000:200
4) On R2:
interface Ethernet0/2.100
mpls ip
!
interface Ethernet0/2.200
mpls ip
!
router bgp 65000
neighbor 10.10.10.1 remote-as 65000
neighbor 10.10.20.1 remote-as 65000
!
address-family vpnv4
neighbor 10.10.10.1 activate
neighbor 10.10.20.1 activate
exit-address-family
!

address-family ipv4 vrf cu-green
redistribute connected
exit-address-family
!
address-family ipv4 vrf cu-red
redistribute connected
exit-address-family
R2(config)#ip vrf cu-red
R2(config-vrf)#route-target both 65000:100
!
R2(config)#ip vrf cu-green
R2(config-vrf)#route-target both 65000:200
5) Verification:
From SW1 to SW3:
SW1#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
But can't Reach SW2 or SW4 in VRF cu-green:
SW1#ping 192.168.22.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.22.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
SW1#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
Same Test for SW2:
From SW2 to SW4:
SW2#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
But can't Reach SW3 or SW1 in VRF cu-red:
SW2#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
SW2#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
Both R1 & R2 has separate tables for VRFs cu-red and cu-green.

388.LAB SIMULATION



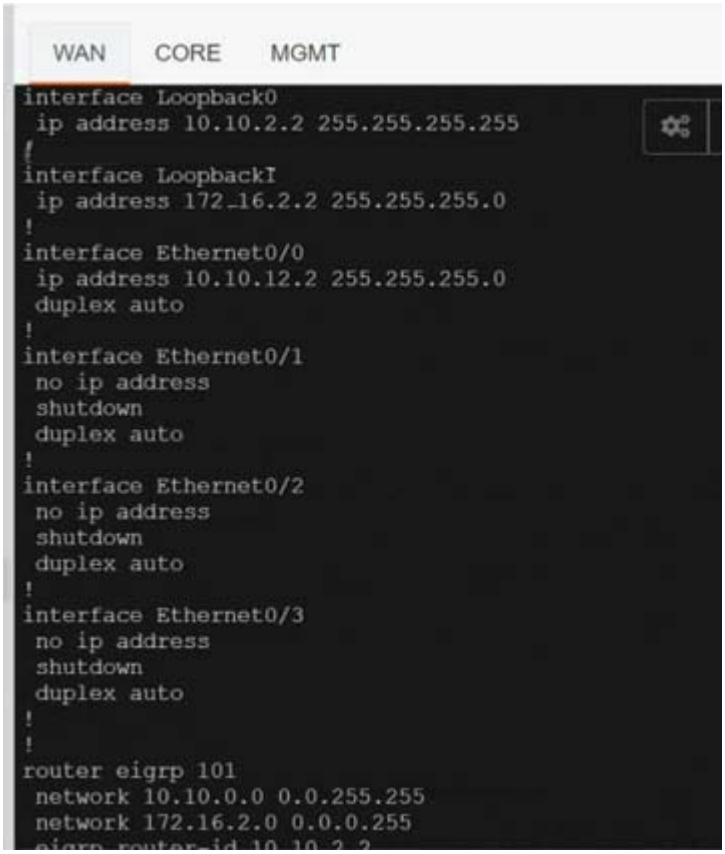
Guidelines Topology Tasks

A network is configured with CoPP to protect the CORE router route processor for stability and DDoS protection. As a company policy, a class named class-default is preconfigured and must not be modified or deleted. Troubleshoot CoPP to resolve the issues introduced during the maintenance window to ensure that:

1. Dynamic routing policies are under CoPP-CRITICAL and are allowed only from the 10.10.x.x range.
2. Telnet, SSH, and ping are under CoPP-IMPORTANT and are allowed strictly to/from 10.10.x.x to the CORE router (Hint: you can verify using Loopback1).
3. All devices ping (UDP) any CORE router interface successfully to/from the 10.10.x.x range and do not allow any other IP address.
   NORMAL (Hint: Traceroute port range 33434 33464).

WAN

```
!
!
interface Loopback0
 ip address 10.10.2.2 255.255.255.255
!
interface Loopback1
 ip address 172.16.2.2 255.255.255.255
!
```




```
!
!
router eigrp 101
 network 10.10.0.0 0.0.255.255
 network 172.16.2.0 0.0.0.255
 eigrp router-id 10.10.2.2
!
```

CORE

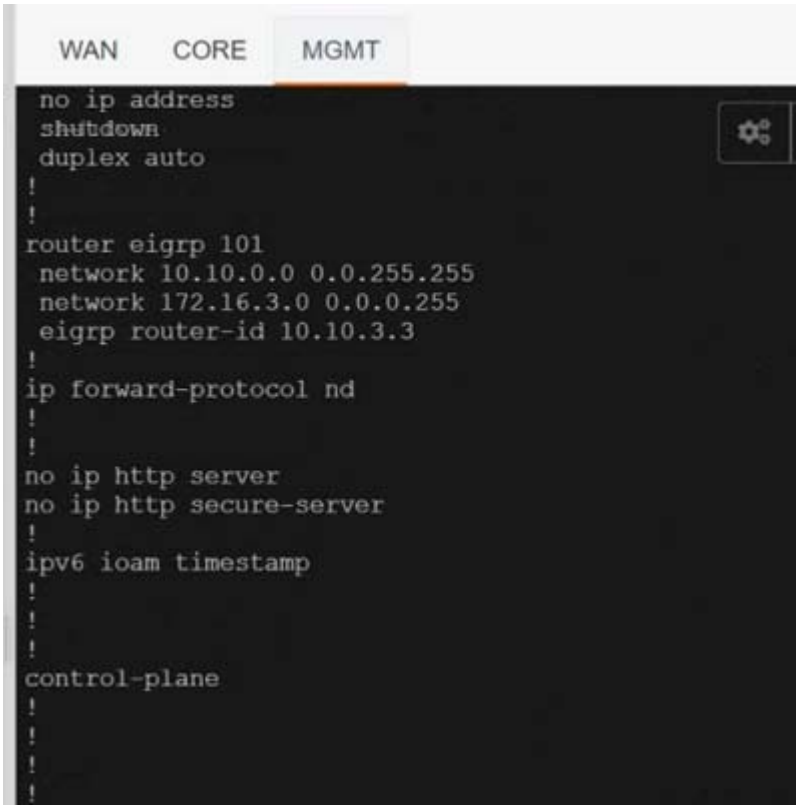
```
!
class-map match-all CoPP-CRITICAL
 match access-group 120
class-map match-all CoPP-NORMAL
 match access-group 122
class-map match-all CoPP-IMPORTANT
 match access-group 121
!
policy-map CoPP
 class CoPP-CRITICAL
  police 1000000 50000 50000 conform-action transmit  exceed
-action drop
 class CoPP-IMPORTANT
  police 100000 20000 20000 conform-action transmit  exceed-
action drop
 class CoPP-NORMAL
  police 64000 6400 64000 conform-action transmit  exceed-ac
tion drop
 class class-default
  police 8000 1500 1500 conform-action drop  exceed-action d
rop
!
```

```
!
interface Loopback0
 ip address 10.10.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 10.10.12.1 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 ip address 10.10.13.1 255.255.255.0
 duplex auto
!
```

```
interface Ethernet0/1
 ip address 10.10.13.1 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
!
router eigrp 101
 network 10.10.0.0 0.0.255.255
 eigrp router-id 10.10.1.1
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure server
!
ipv6 ioam timestamp
```

```
!
!
access-list 120 remark *** ACL for CoPP-Critical ***
access-list 121 remark *** ACL for CoPP-IMPORTANT
access-list 122 remark *** ACL for CoPP-NORMAL
!
control-plane
 service-policy input CoPP
!
```

MGMT



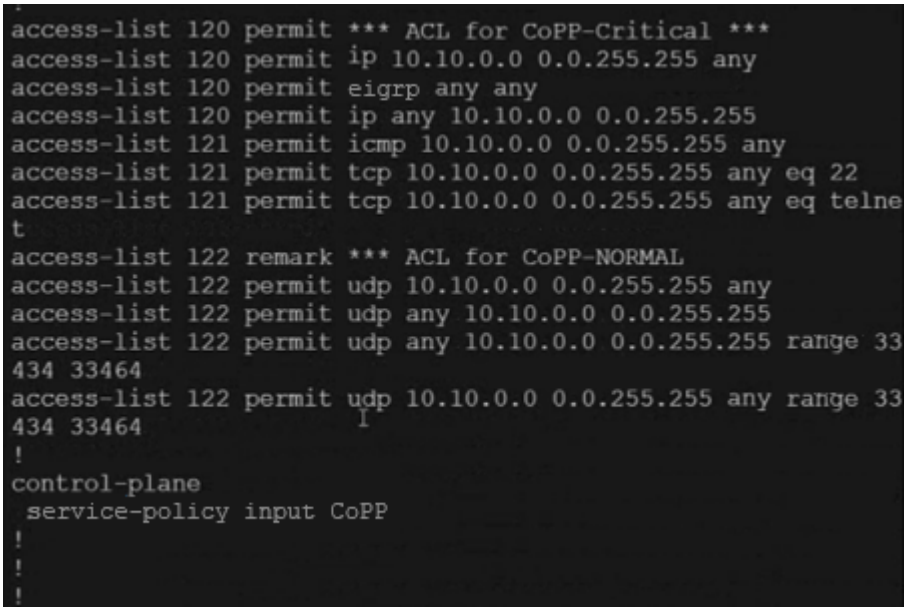
Answer:

CORE

policy-mao CoPP

class CoPP-CRITICAL

police 1000000 50000 50000 conform-action transmit exceed-action transmit



CORE# Copy run start

TESTING: -

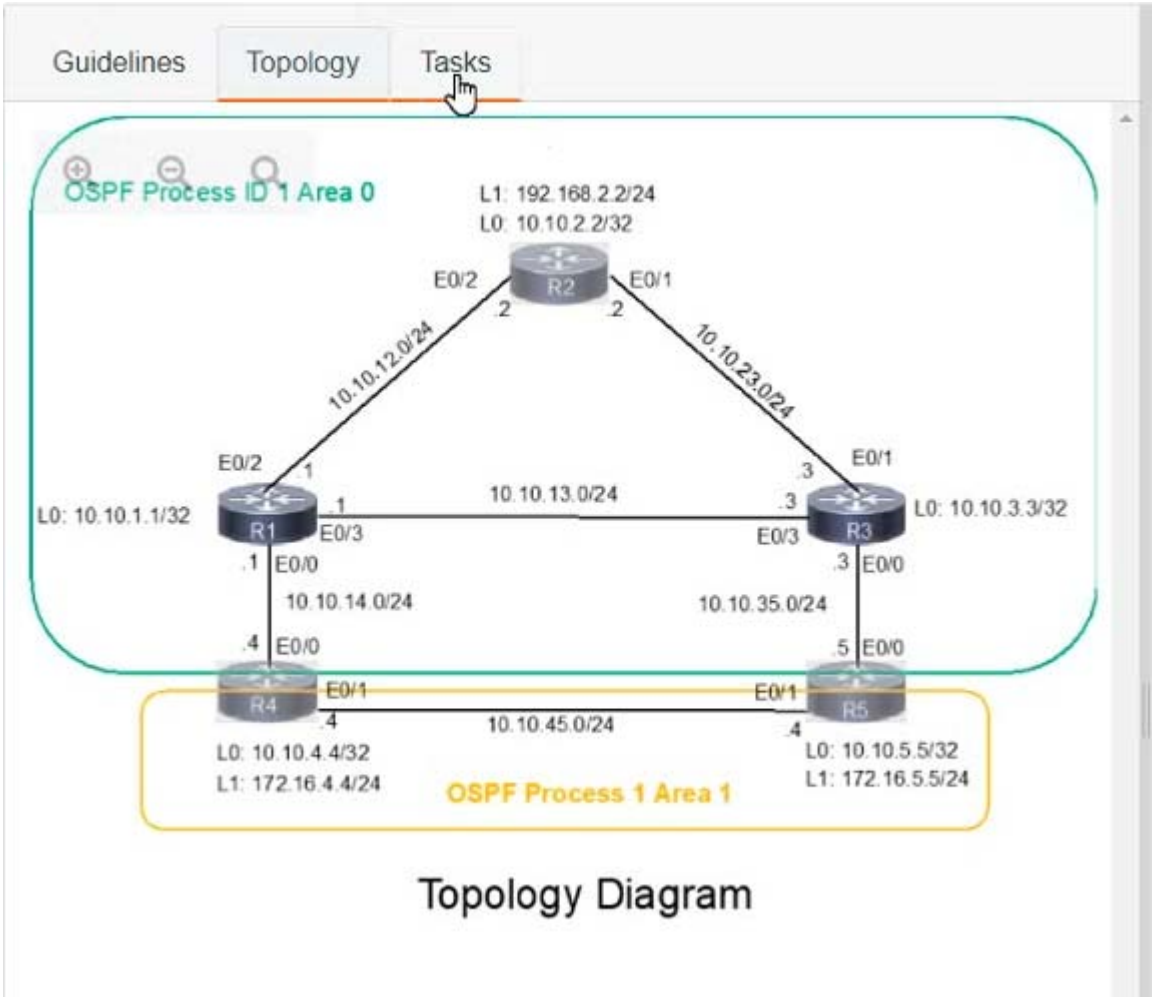
CORE

```
CORE#sh ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(101)
H   Address                 Interface              Hold Upti
me   SRTT   RTO  Q  Seq
                                                   (sec)
     (ms)       Cnt Num
0   10.10.13.3              Et0/1                    11 00:0
3:15    5   100  0  35
1   10.10.12.2              Et0/0                    11 00:0
3:24    7   100  0  33
CORE#copy run star
```

MGMT

```
MGMT#telnet 10.10.13.1
Trying 10.10.13.1 ...
% Connection refused by cemote host

MGMT#telnet 10.10.13.1
Trying 10.10.13.1 ... Open


Password required, but none set

[Connection to 10.10.13.1 closed by forcign hostl
MGMT#
```

389.LAB SIMULATION

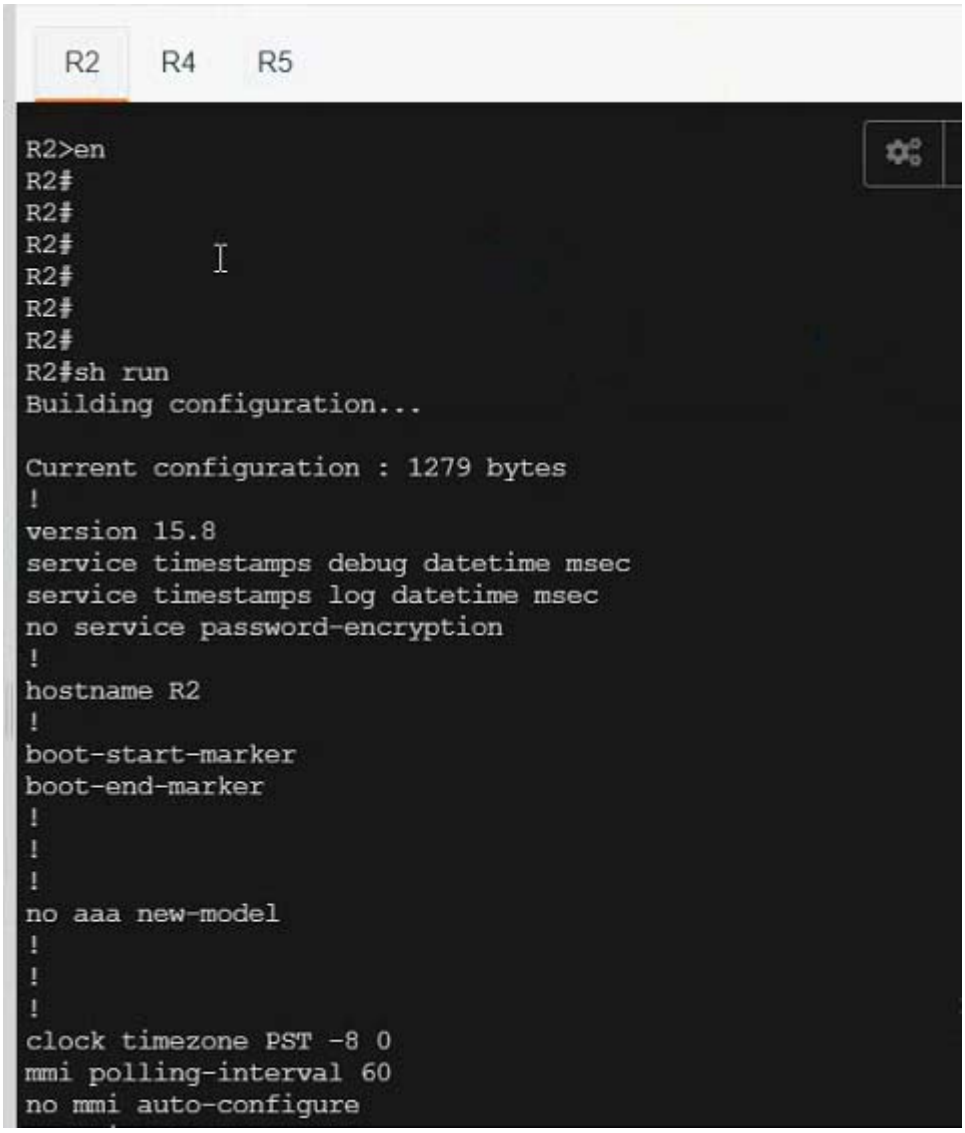


Topology Diagram

Guidelines Topology Tasks

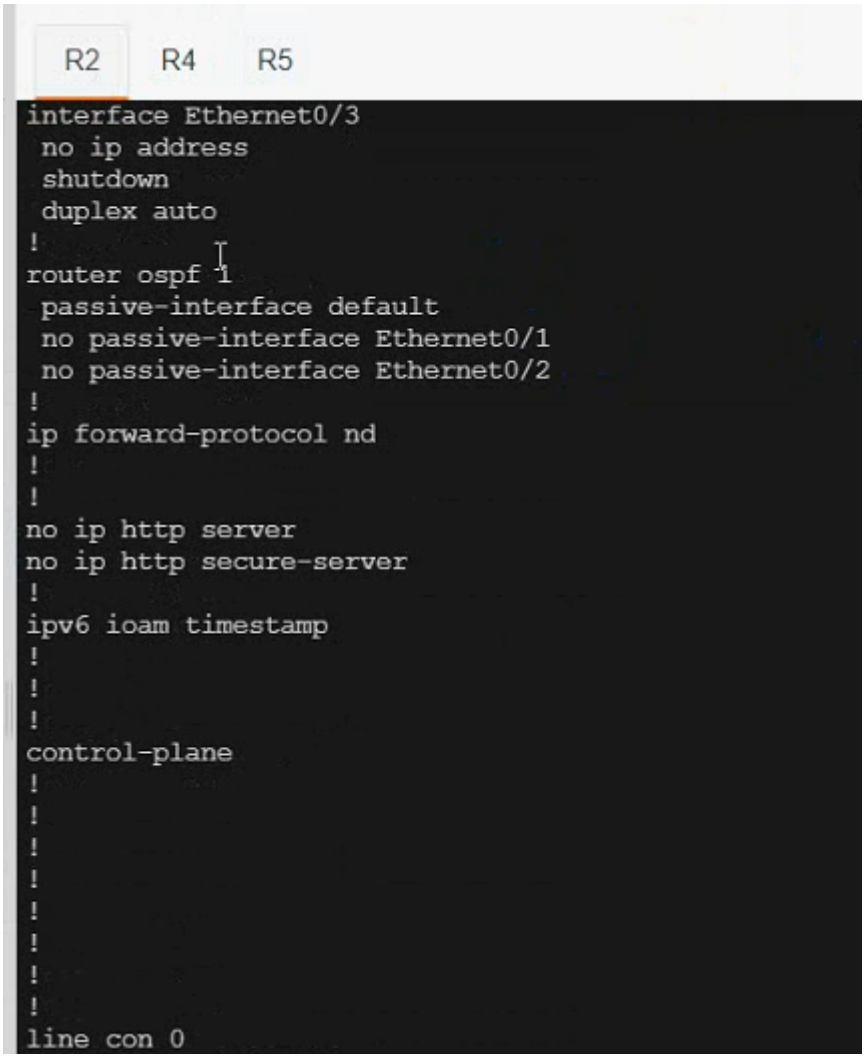
A network is configured with IP connectivity, and the routing protocol between devices started having problems right after the maintenance window to implement network changes. Troubleshoot and resolve to a fully functional network to ensure that:

1. Inter-area links have link authentication (not area authentication) using MD5 with the key 1 string CCNP.
2. R3 is a DR regardless of R2 status while R1 and R2 establish a DR/BDR relationship.
3. OSPF uses the default cost on all interfaces. Network reachability must follow OSPF default behavior for traffic within an area over intra-area VS inter-area links.
4. The OSPF external route generated on R4 adds link cost when traversing through the network to reach R2. A network command to advertise routes is not allowed.

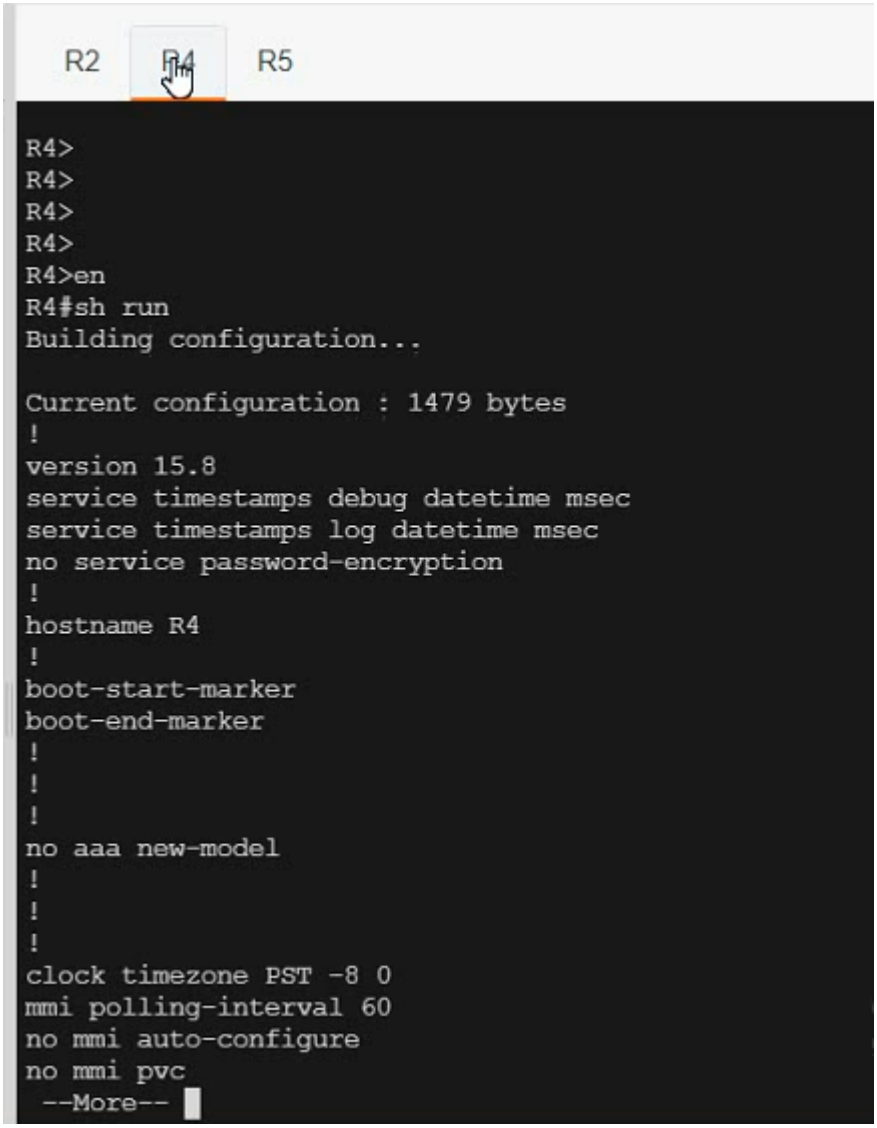

R2
R4
R5
R2>en
R2#
R2#
R2#
R2#
R2#
R2#
R2#sh run
Building configuration...
Current configuration : 1279 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure

R2 R4 R5

```
interface Loopback0
 ip address 10.10.2.2 255.255.255.255
 ip ospf 1 area 0
!
interface Loopback1
 ip address 192.168.2.2 255.255.255.0
 ip ospf 1 area 0
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/1
 ip address 10.10.23.2 255.255.255.0
 ip ospf 1 area 0
 duplex auto
!
interface Ethernet0/2
 ip address 10.10.12.2 255.255.255.0
 ip ospf 1 area 0
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
router ospf 1
 passive-interface default
 no passive-interface Ethernet0/1
 no passive-interface Ethernet0/2
```

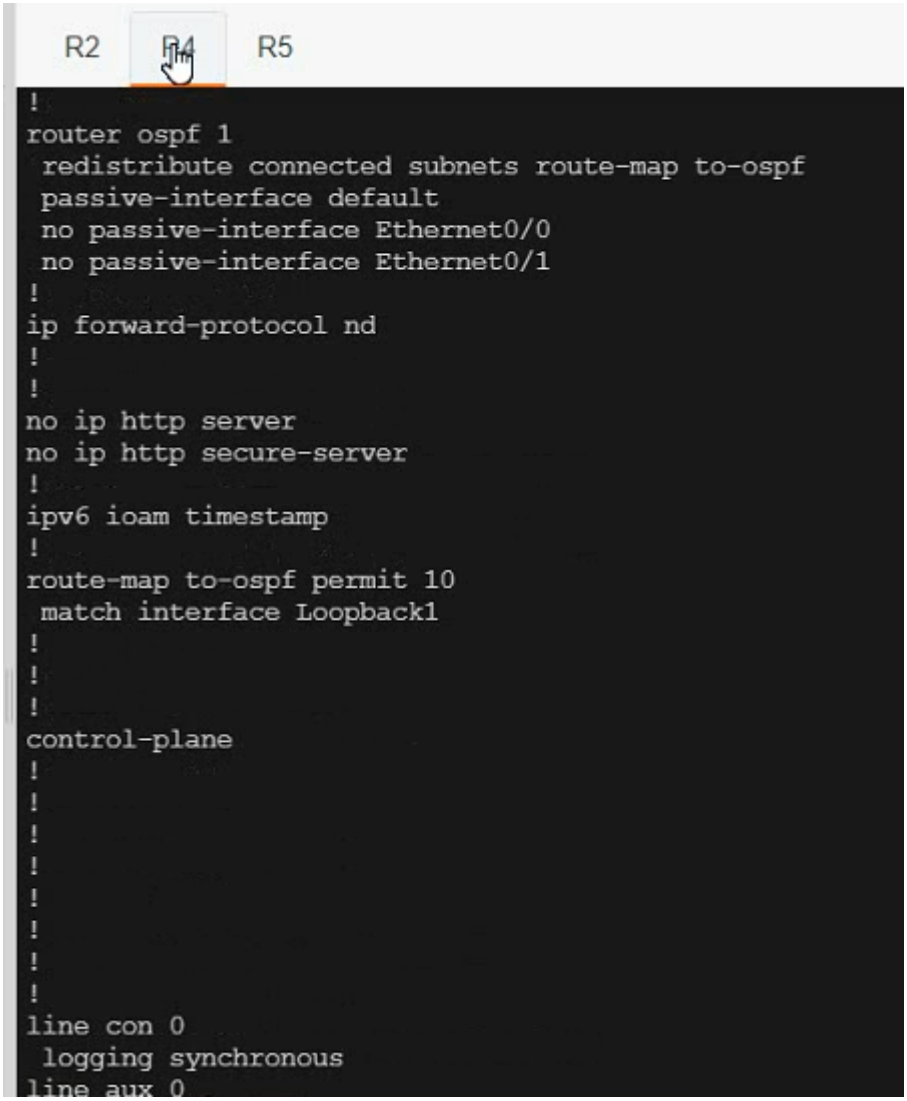

R2
R4
R5
interface Ethernet0/3
no ip address
shutdown
duplex auto
!
router ospf 1
passive-interface default
no passive-interface Ethernet0/1
no passive-interface Ethernet0/2
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0

R4

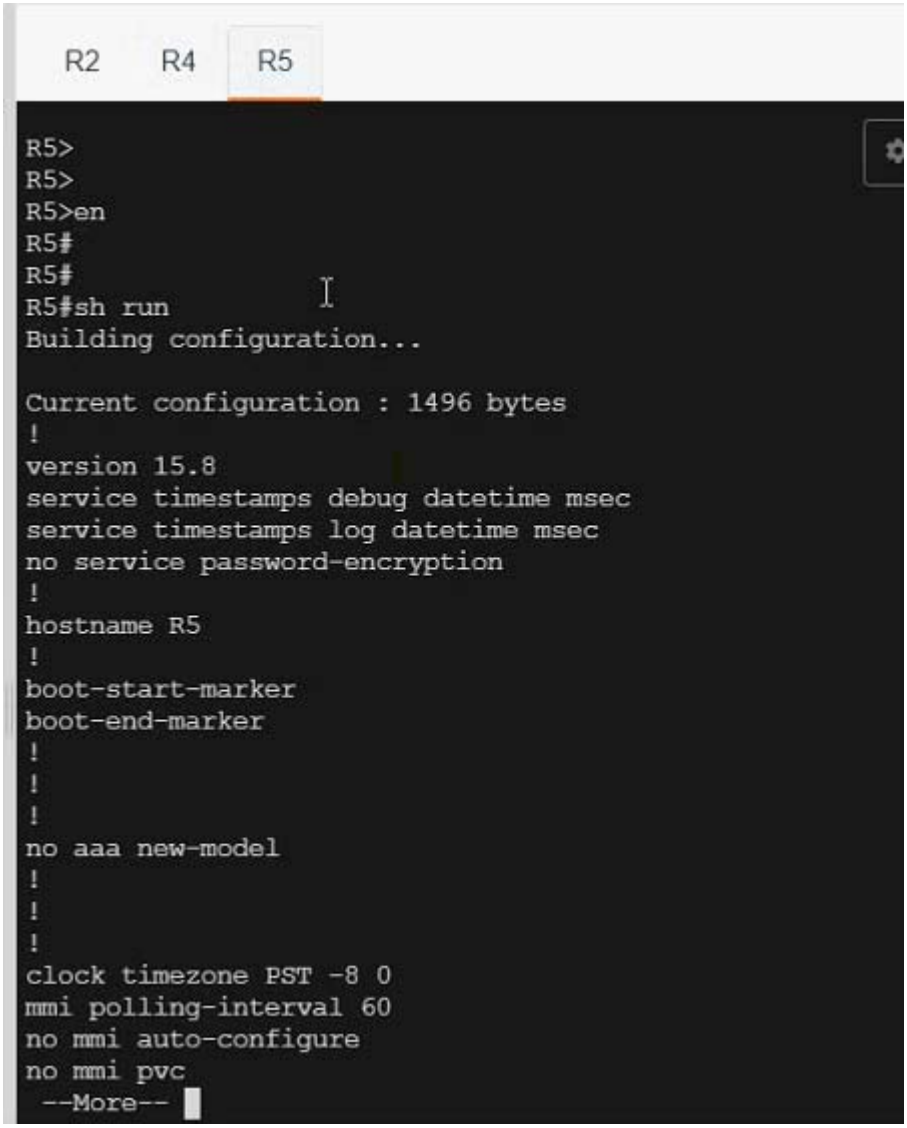

R2
R4
R5
R4>
R4>
R4>
R4>
R4>en
R4#sh run
Building configuration...
Current configuration : 1479 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
--More--

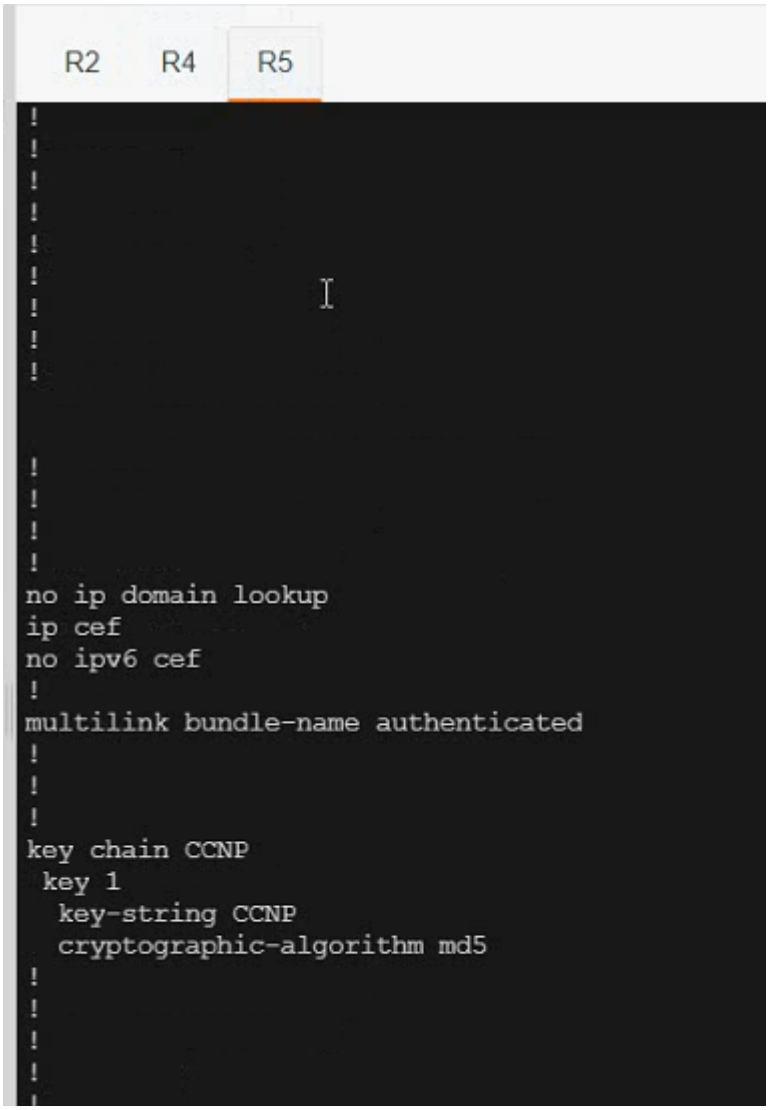
R2 R4 R5

```
key chain CCNP
 key 1
  key-string ccnp
  cryptographic-algorithm md5
!
!
!
!
!
!
 ip address 172.16.4.4 255.255.255.0
!
interface Ethernet0/0
 ip address 10.10.14.4 255.255.255.0
 ip ospf authentication key-chain CCNP
 ip ospf 1 area 0
 duplex auto
!
interface Ethernet0/1
 ip address 172.16.45.4 255.255.255.0
 ip ospf 1 area 1
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
```


R2
R4
R5
!
router ospf 1
redistribute connected subnets route-map to-ospf
passive-interface default
no passive-interface Ethernet0/0
no passive-interface Ethernet0/1
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ipv6 ioam timestamp
!
route-map to-ospf permit 10
match interface Loopback1
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
logging synchronous
line aux 0

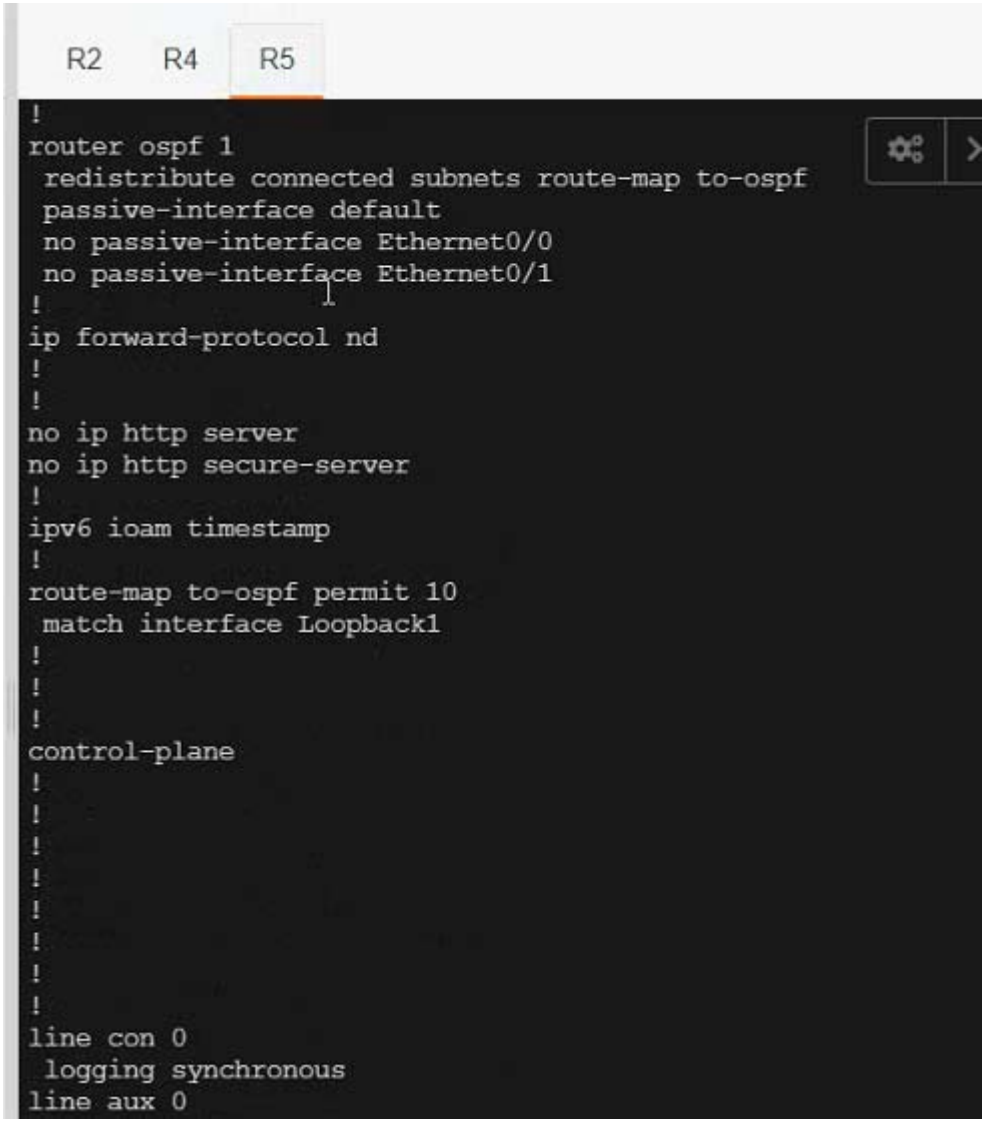
R5


R2
R4
R5
R5>
R5>
R5>en
R5#
R5#
R5#sh run
Building configuration...
Current configuration : 1496 bytes
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R5
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
clock timezone PST -8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
--More--


R2
R4
R5
!
!
!
!
!
!
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
key chain CCNP
key 1
key-string CCNP
cryptographic-algorithm md5
!
!
!
!

R2 R4 R5

```
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.5.5 255.255.255.255
 ip ospf 1 area 1
!
interface Loopback1
 ip address 172.16.5.5 255.255.255.0
!
interface Ethernet0/0
 ip address 10.10.35.5 255.255.255.0
 ip ospf authentication key-chain CCNP
 ip ospf 1 area 0
 duplex auto
!
interface Ethernet0/1
 ip address 172.16.45.5 255.255.255.0
 ip ospf 1 area 1
 ip ospf cost 60
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
```



Answer:

R4

Int range et0/0 – 1

Ip ospf authentication message-digest

Ip ospf message-digest-key 1 md5 CCNP

Router ospf 1

Redistribute connected subnets route-map to-ospf metric-type 1

Copy run start

R5

Int range et0/0 – 1

Ip ospf authentication message-digest

Ip ospf message-digest-key 1 md5 CCNP

Interface eth 0/1

Ip ospf cost 10

Copy run start

VERIFICATION: -

```
R2#show ip ospf nei
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         I
nterface
10.10.1.1         1   FULL/BDR        00:00:38    10.10.12.1      E
thernet0/2
10.10.3.3         1   FULL/BDR        00:00:30    10.10.23.3      E
thernet0/1
R2#
```

390.What are two characteristics of a VRF instance? (Choose two)
A. It is defined by the VPN membership of a customer site attached to a P device.
B. Each VRF has a different set of routing and CEF tables.
C. AII VRFS share customers routing and CEF tables.
D. An interface must be associated to one VRF
E. A customer site can be associated to different VRFs.
Answer: BD

391.The network administrator configured CoPP so that all routing protocol traffic toward the router CPU is limited to 1 mbps. All traffic that exceeds this limit must be dropped.
The router is running BGP and OSPF Management traffic for Telnet and SSH
must be limited to 500kbps.
access-list 100 permit tcp any any eq 179
access-list 100 permit tcp any any range 22 23
access-list 100 permit ospf any any
!
class-map CM-ROUTING
match access-group 100
class-map CM-MGMT
match access-group 100
!
policy-map PM-COPP
class CM-ROUTING
police 1000000 conform-action transmit
class CM-MGMT
police 500000 conform-action transmit
!
control-plane
service-policy output PM-COPP
No traffic is filtering through CoPP,which is resulting in high CPU utilization,
Which configuration resolves
the issue?
A. no access-list 100access-list 100 permit tcp any any eq 179
access-list 100 permit ospf any any
access-list 101 Permit tcp any any range 22 23

!
class-map CM-MGMT
no match access-group 100
match access-group 101
B. control-plane
no service-policy output PM-COPP
service-policy input PM-COPP
C. No access-list 100
access-list 100 permit tcp any any eq 179
access-list 100 permit tcp any any range eq 22
access-list 100 permit tcp any any range eq 23
access-list 100 permit ospf any any
D. no access-list 100
access-list 100 permit tcp any any eq 179
access-list 100 permit ospf any any
access-list 101 Permit tcp any any range 22 23
!
class-map CM-MGMT
no match access-group 100
match access-group 101
!
control-plane
no service-policy output PM-COPP
service-policy input PM-COPP
Answer: D

392.An engineer is creating a policy that overrides normal routing behavior. If the route to a destination of 10.100.100.0/24 is withdrawn from the routing Table, the policy must direct traffic to a next hop of 10.1 1.1. if the route is present in the routing table, then normal forwarding must occur.
Which configuration meets the requirements?
A. access-list 100 permit ip any any
!
route-map POLICY permit 10
match ip address 100
set ip next-hop recursive 10.1.1.1
B. access-list 100 permit ip any 10.100.100.0 0.0.0.255
!
Route-map POLICY permit 10
match ip address 100
set ip default next-hop 10.1.1.1
C. access-list 100 permit ip any 10.100.100.0 0.0.0.255
!
route-map POLICY permit 10
match ip address 100

set ip next-hop 10.1.1.1
!
route map POLICY permit 20
D. access-list 100 permit ip any 10.100.100.0 0.0.0.255
!
route map POLICY permit 10
match ip address 100
Set ip next-hop recursive 10.1.1.1
!
route-map POLICY permit 20
Answer: D

393.Refer to the exhibit.

```
Dallas_Router:

interface GigabitEthernet0/0/0.364
 description Guest_Wifi_10.66.46.0/23
 encapsulation dot1Q 364
 ip address 10.66.46.1 255.255.254.0
 ip helper-address 10.192.104.212
 ip helper-address 10.191.103.140
 ip access-group GUEST-ACCESS in
 ip access-group GUEST-ACCESS-OUT out
 no ip redirects
 no ip unreachables
 no ip proxy-arp

ip access-list extended GUEST-ACCESS
 remark Internet Access Only
 permit udp any any eq bootpc
 permit udp any any eq bootps
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 deny   ip any 224.0.0.0 31.255.255.255
 deny   ip any 169.254.0.0 0.0.255.255
 deny   ip any 127.0.0.0 0.255.255.255
 deny   ip any 192.0.2.0 0.0.0.255
 deny   ip any host 0.0.0.0
 permit ip 10.66.42.0 0.0.0.255 any
 permit ip 10.66.46.0 0.0.0.255 any
!
ip access-list extended GUEST-ACCESS-OUT
 remark Used to block inbound traffic to Guest Networks
 permit udp any any eq bootps
 permit udp any any eq bootpc
 permit udp any any eq domain
 permit udp any any
 permit icmp any any
 permit tcp host 10.192.103.124 eq 15871 any
 permit tcp any any established
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 deny   ip any 224.0.0.0 31.255.255.255
 deny   ip any 169.254.0.0 0.0.255.255
 deny   ip any 127.0.0.0 0.255.255.255
 deny   ip any 192.0.2.0 0.0.0.255
 deny   ip any host 0.0.0.0
```

After a new regional office is set up, not all guests can access the internet via guest WiFi. Clients are getting the correct IP address from guest Wi-Fi VLAN 364.

Which action resolves the issue?

A. Allow 10.66.46.0/23 in the outbound ACL

B. Allow DNS traffic through the outbound ACL

C. Allow DNS traffic through the inbound ACL

D. Allow 10.66.46.0/23 in the inbound ACL

Answer: C

394.An engineer configures PBR on R5 and wants to create a policy that matches traffic destined toward 10.10.10.0/24 and forward 10.1.1.1. The traffic must also have its IP precedence set to 5. All other traffic should be forward toward 10.1.1.2 and have its IP precedence set to 0.
Which configuration meets the requirements?
A. access-list 1 permit 10.10.10.0 0.0.0.255
access-list 2 permit any
route-map CCNP permit 10
match ip address 1
set ip next-hop 10.1.1.1
set ip precedence 5
!
route-map CCNP permit 20
match ip address 2
set ip next-hop 10.1.1.2
set ip precedence 0route-map CCNP permit 30
B. access-list 100 permit ip any 10.10.10.0 0.0.0.255
route-map CCNP permit 10
match ip address 100
set ip next-hop 10.1.1.1
set ip precedence 0
!
route-map CCNP permit 20
set ip next-hop 10.1.1.2
set ip precedence 5
!
route-map CCNP permit 30
C. access-list 1 permit 10.10.10.0 0.0.0.255
route-map CCNP permit 10
match ip address 1
set ip next-hop 10.1.1.1
set ip precedence 5
!
route-map CCNP permit 20
set ip next-hop 10.1.1.2
set ip precedence 0
D. access-list 100 permit ip any 10.10.10.0 0.0.0.255
route-map CCNP permit 10
match ip address 100
set ip next-hop 10.1.1.1
set ip precedence 5
!
route-map CCNP permit 20
set ip next-hop 10.1.1.2

set ip precedence 0
Answer: D